Policy and Procedures (AC-1)

Description for Policy and Procedures (AC-1)
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] access control policy that:
(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the access control policy and the associated access controls;
b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the access control policy and procedures; and
c. Review and update the current access control:
1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

Discussion for Policy and Procedures (AC-1)
Access control policy and procedures address the controls in the AC family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of access control policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies reflecting the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, 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. Events that may precipitate an update to access control policy and procedures include assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Account Management (AC-2)

Description for Account Management (AC-2)
a. Define and document the types of accounts allowed and specifically prohibited for use within the system;
b. Assign account managers;
c. Require [Assignment: organization-defined prerequisites and criteria] for group and role membership;
d. Specify:
1. Authorized users of the system;
2. Group and role membership; and
3. Access authorizations (i.e., privileges) and [Assignment: organization-defined attributes (as required)] for each account;
e. Require approvals by [Assignment: organization-defined personnel or roles] for requests to create accounts;
f. Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, prerequisites, and criteria];
g. Monitor the use of accounts;
h. Notify account managers and [Assignment: organization-defined personnel or roles] within:
1. [Assignment: organization-defined time period] when accounts are no longer required;
2. [Assignment: organization-defined time period] when users are terminated or transferred; and
3. [Assignment: organization-defined time period] when system usage or need-to-know changes for an individual;
i. Authorize access to the system based on:
1. A valid access authorization;
2. Intended system usage; and
3. [Assignment: organization-defined attributes (as required)];
j. Review accounts for compliance with account management requirements [Assignment: organization-defined frequency];
k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and
l. Align account management processes with personnel termination and transfer processes.

Discussion for Account Management (AC-2)
Examples of system account types include individual, shared, group, system, guest, anonymous, emergency, developer, temporary, and service. Identification of authorized system users and the specification of access privileges reflect the requirements in other controls in the security plan. Users requiring administrative privileges on system accounts receive additional scrutiny by organizational personnel responsible for approving such accounts and privileged access, including

system owner, mission or business owner, senior agency information security officer, or senior agency official for privacy. Types of accounts that organizations may wish to prohibit due to increased risk include shared, group, emergency, anonymous, temporary, and guest accounts.

Where access involves personally identifiable information, security programs collaborate with the senior agency official for privacy to establish the specific conditions for group and role membership; specify authorized users, group and role membership, and access authorizations for each account; and create, adjust, or remove system accounts in accordance with organizational policies. Policies can include such information as account expiration dates or other factors that trigger the disabling of accounts. Organizations may choose to define access privileges or other attributes by account, type of account, or a combination of the two. Examples of other attributes required for authorizing access include restrictions on time of day, day of week, and point of origin. In defining other system account attributes, organizations consider system-related requirements and mission/business requirements. Failure to consider these factors could affect system availability.

Temporary and emergency accounts are intended for short-term use. Organizations establish temporary accounts as part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation. Organizations establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes. Emergency and temporary accounts are not to be confused with infrequently used accounts, including local logon accounts used for special tasks or when network resources are unavailable (may also be known as accounts of last resort). Such accounts remain available and are not subject to automatic disabling or removal dates. Conditions for disabling or deactivating accounts include when shared/group, emergency, or temporary accounts are no longer required and when individuals are transferred or terminated. Changing shared/group authenticators when members leave the group is intended to ensure that former group members do not retain access to the shared or group account. Some types of system accounts may require specialized training.

Account Management | Automated System Account Management (AC-2(1))

Description for Account Management | Automated System Account Management (AC-2(1))
Support the management of system accounts using [Assignment: organization-defined automated mechanisms].

Discussion for Account Management | Automated System Account Management (AC-2(1))
Automated system account management includes using automated mechanisms to create, enable, modify, disable, and remove accounts; notify account managers when an account is created, enabled, modified, disabled, or removed, or when users are terminated or transferred; monitor system account usage; and report atypical system account usage. Automated mechanisms can include internal system functions and email, telephonic, and text messaging notifications.

Account Management | Automated Temporary and Emergency Account Management (AC-2(2))

Description for Account Management | Automated Temporary and Emergency Account Management (AC-2(2))
Automatically [Selection: remove; disable] temporary and emergency accounts after [Assignment: organization-defined time period for each type of account].

Discussion for Account Management | Automated Temporary and Emergency Account Management (AC-2(2))
Management of temporary and emergency accounts includes the removal or disabling of such accounts automatically after a predefined time period rather than at the convenience of the system administrator. Automatic removal or disabling of accounts provides a more consistent implementation.

Account Management | Disable Accounts (AC-2(3))

Description for Account Management | Disable Accounts (AC-2(3))
Disable accounts within [Assignment: organization-defined time period] when the accounts:
(a) Have expired;
(b) Are no longer associated with a user or individual;
(c) Are in violation of organizational policy; or
(d) Have been inactive for [Assignment: organization-defined time period].

Discussion for Account Management | Disable Accounts (AC-2(3))
Disabling expired, inactive, or otherwise anomalous accounts supports the concepts of least privilege and least functionality which reduce the attack surface of the system.

Account Management | Automated Audit Actions (AC-2(4))

Description for Account Management | Automated Audit Actions (AC-2(4))
Automatically audit account creation, modification, enabling, disabling, and removal actions.

Discussion for Account Management | Automated Audit Actions (AC-2(4))
Account management audit records are defined in accordance with AU-2 and reviewed, analyzed, and reported in accordance with AU-6.

Account Management | Inactivity Logout (AC-2(5))

Description for Account Management | Inactivity Logout (AC-2(5))
Require that users log out when [Assignment: organization-defined time period of expected inactivity or description of when to log out].

Discussion for Account Management | Inactivity Logout (AC-2(5))
Inactivity logout is behavior- or policy-based and requires users to take physical action to log out when they are expecting inactivity longer than the defined period. Automatic enforcement of inactivity logout is addressed by AC-11.

Account Management | Dynamic Privilege Management (AC-2(6))

Description for Account Management | Dynamic Privilege Management (AC-2(6))
Implement [Assignment: organization-defined dynamic privilege management capabilities].

Discussion for Account Management | Dynamic Privilege Management (AC-2(6))
In contrast to access control approaches that employ static accounts and predefined user privileges, dynamic access control approaches rely on runtime 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 based on ongoing mission or business requirements and the operational needs of organizations. An example of dynamic privilege management is the immediate revocation of privileges from users as opposed to requiring that users terminate and restart their sessions to reflect changes in privileges. Dynamic privilege management can also include mechanisms that change user privileges based on dynamic rules as opposed to editing specific user profiles. Examples include automatic adjustments of user privileges if they are operating out of their normal work times, if their job function or assignment changes, or if systems are under duress or in emergency situations. Dynamic privilege management includes the effects of privilege

changes, for example, when there are changes to encryption keys used for communications.

Account Management | Privileged User Accounts (AC-2(7))

Description for Account Management | Privileged User Accounts (AC-2(7))
(a) Establish and administer privileged user accounts in accordance with [Selection: a role-based access scheme; an attribute-based access scheme];
(b) Monitor privileged role or attribute assignments;
(c) Monitor changes to roles or attributes; and
(d) Revoke access when privileged role or attribute assignments are no longer appropriate.

Discussion for Account Management | Privileged User Accounts (AC-2(7))
Privileged roles are organization-defined roles assigned to individuals that allow those individuals to perform certain security-relevant functions that ordinary users are not authorized to perform. Privileged roles include key management, account management, database administration, system and network administration, and web administration. A role-based access scheme organizes permitted system access and privileges into roles. In contrast, an attribute-based access scheme specifies allowed system access and privileges based on attributes.

Account Management | Dynamic Account Management (AC-2(8))

Description for Account Management | Dynamic Account Management (AC-2(8))
Create, activate, manage, and deactivate [Assignment: organization-defined system accounts] dynamically.

Discussion for Account Management | Dynamic Account Management (AC-2(8))
Approaches for dynamically creating, activating, managing, and deactivating system accounts rely on automatically provisioning the accounts at runtime for entities that were previously unknown. Organizations plan for the dynamic management, creation, activation, and deactivation of system accounts by establishing trust relationships, business rules, and mechanisms with appropriate authorities to validate related authorizations and privileges.

Account Management | Restrictions on Use of Shared and Group Accounts (AC-2(9))

Description for Account Management | Restrictions on Use of Shared and Group Accounts (AC-2(9))
Only permit the use of shared and group accounts that meet [Assignment: organization-defined conditions for establishing shared and group accounts].

Discussion for Account Management | Restrictions on Use of Shared and Group Accounts (AC-2(9))
Before permitting the use of shared or group accounts, organizations consider the increased risk due to the lack of accountability with such accounts.

Supervision and Review — Access Control (AC-13)

Description for Supervision and Review — Access Control (AC-13)
[Withdrawn: Incorporated into AC-2 and AU-6.]

Discussion for Supervision and Review — Access Control (AC-13)

Account Management | Usage Conditions (AC-2(11))

Description for Account Management | Usage Conditions (AC-2(11))
Enforce [Assignment: organization-defined circumstances and/or usage conditions] for [Assignment: organization-defined system accounts].

Discussion for Account Management | Usage Conditions (AC-2(11))
Specifying and enforcing usage conditions helps to enforce the principle of least privilege, increase user accountability, and enable effective account monitoring. Account monitoring includes alerts generated if the account is used in violation of organizational parameters. Organizations can describe specific conditions or circumstances under which system accounts can be used, such as by restricting usage to certain days of the week, time of day, or specific durations of time.

Account Management | Account Monitoring for Atypical Usage (AC-2(12))

Description for Account Management | Account Monitoring for Atypical Usage (AC-2(12))
(a) Monitor system accounts for [Assignment: organization-defined atypical usage]; and
(b) Report atypical usage of system accounts to [Assignment: organization-defined personnel or roles].

Discussion for Account Management | Account Monitoring for Atypical Usage (AC-2(12))
Atypical usage includes accessing systems at certain times of the day or from locations that are not consistent with the normal usage patterns of individuals. Monitoring for atypical usage may reveal rogue behavior by individuals or an attack in progress. Account monitoring may inadvertently create privacy risks since data collected to identify atypical usage may reveal previously unknown information about the behavior of individuals. Organizations assess and document privacy risks from monitoring accounts for atypical usage in their privacy impact assessment and make determinations that are in alignment with their privacy program plan.

Account Management | Disable Accounts for High-risk Individuals (AC-2(13))

Description for Account Management | Disable Accounts for High-risk Individuals (AC-2(13))
Disable accounts of individuals within [Assignment: organization-defined time period] of discovery of [Assignment: organization-defined significant risks].

Discussion for Account Management | Disable Accounts for High-risk Individuals (AC-2(13))
Users who pose a significant security and/or privacy risk include individuals for whom reliable evidence indicates either the intention to use authorized access to systems to cause harm or through whom adversaries will cause harm. Such harm includes adverse impacts to organizational operations, organizational assets, individuals, other organizations, or the Nation. Close coordination among system administrators, legal staff, human resource managers, and authorizing officials is essential when disabling system accounts for high-risk individuals.

Access Enforcement (AC-3)

Description for Access Enforcement (AC-3)
Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

Discussion for Access Enforcement (AC-3)
Access control policies control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (i.e., devices, files, records, domains) in organizational systems. In addition to enforcing authorized access at the system level and recognizing that systems can host many applications and services in support of mission 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.

Permitted Actions Without Identification or Authentication | Necessary Uses (AC-14(1))

Description for Permitted Actions Without Identification or Authentication | Necessary Uses (AC-14(1))
[Withdrawn: Incorporated into AC-14.]

Discussion for Permitted Actions Without Identification or Authentication | Necessary Uses (AC-14(1))

Access Enforcement | Dual Authorization (AC-3(2))

Description for Access Enforcement | Dual Authorization (AC-3(2))
Enforce dual authorization for [Assignment: organization-defined privileged commands and/or other organization-defined actions].

Discussion for Access Enforcement | Dual Authorization (AC-3(2))
Dual authorization, also known as two-person control, reduces risk related to insider threats. Dual authorization mechanisms require the approval of two authorized individuals to execute. To reduce the risk of collusion, organizations consider rotating dual authorization duties. Organizations consider the risk associated with implementing dual authorization mechanisms when immediate responses are necessary to ensure public and environmental safety.

Access Enforcement | Mandatory Access Control (AC-3(3))

Description for Access Enforcement | Mandatory Access Control (AC-3(3))
Enforce [Assignment: organization-defined mandatory access control policy] over 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 subjects or objects;
(2) Granting 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) Choosing the security attributes and attribute values (specified by the policy) to be associated with newly created or modified objects; and
(5) Changing the rules governing access control; and
(c) Specifies that [Assignment: organization-defined subjects] may explicitly be granted [Assignment: organization-defined privileges] such that they are not limited by any defined subset (or all) of the above constraints.

Discussion for Access Enforcement | Mandatory Access Control (AC-3(3))
Mandatory access control is a type of nondiscretionary access control. Mandatory access control policies constrain what actions subjects can take with information obtained from objects for which they have already been granted access. This prevents the subjects from passing the information to unauthorized subjects and objects. Mandatory access control policies constrain actions that subjects can take with respect to the propagation of access control privileges; that is, a subject with a privilege cannot pass that privilege to other subjects. The policy is uniformly

enforced over all 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 monitor concept as described in AC-25. The policy is bounded by the system (i.e., once the information is passed outside of the control of the system, additional means may be required to ensure that the constraints on the information remain in effect).
The trusted subjects described above are granted privileges consistent with the concept of least privilege (see AC-6). Trusted subjects are only given the minimum privileges necessary for satisfying organizational mission/business needs relative to the above policy. The control is most applicable when there is a mandate that establishes a policy regarding access to controlled unclassified information or classified information and some users of the system are not authorized access to all such information resident in the system. Mandatory access control can operate in conjunction with discretionary access control as described in AC-3(4). A subject constrained in its operation by mandatory access control policies can still operate under the less rigorous constraints of AC-3(4), but mandatory access control policies take precedence over the less rigorous constraints of AC-3(4). For example, while a mandatory access control policy imposes a constraint that prevents a subject from passing information to another subject operating at a different impact or classification level, AC-3(4) permits the subject to pass the information to any other subject with the same impact or classification level as the subject. Examples of mandatory access control policies include the Bell-LaPadula policy to protect confidentiality of information and the Biba policy to protect the integrity of information.

Access Enforcement | Discretionary Access Control (AC-3(4))

Description for Access Enforcement | Discretionary Access Control (AC-3(4))
Enforce [Assignment: organization-defined discretionary access control policy] over the set of covered subjects and objects specified in the policy, and where the policy specifies that a subject that has been granted access to information can do one or more of the following:
(a) Pass the information to any other subjects or objects;
(b) Grant its privileges to other subjects;
(c) Change security attributes on subjects, objects, the system, or the system's components;
(d) Choose the security attributes to be associated with newly created or revised objects; or
(e) Change the rules governing access control.

Discussion for Access Enforcement | Discretionary Access Control (AC-3(4))
When discretionary access control policies are implemented, subjects are not constrained with regard to what actions they can take with information for which they have already been granted access. 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(3) and AC-3(15). 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, while AC-3(3) imposes constraints that prevent a subject from passing information to another subject operating at a different impact or classification level, AC-3(4) permits the subject to pass the information to any subject at the same impact or classification 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, that limitation is not required for this particular use of discretionary access control.

Access Enforcement | Security-relevant Information (AC-3(5))

Description for Access Enforcement | Security-relevant Information (AC-3(5))
Prevent access to [Assignment: organization-defined security-relevant information] except during secure, non-operable system states.

Discussion for Access Enforcement | Security-relevant Information (AC-3(5))
Security-relevant information is information within systems that can potentially impact the operation of security functions or the provision of security services in a manner that could result in failure to enforce system security and privacy policies or maintain the separation of code and data. Security-relevant information includes access control lists, filtering rules for routers or firewalls, configuration parameters for security services, and cryptographic key management information. Secure, non-operable system states include the times in which systems are not performing mission or business-related processing, such as when the system is offline for maintenance, boot-up, troubleshooting, or shut down.

Automated Marking (AC-15)

Description for Automated Marking (AC-15)
[Withdrawn: Incorporated into MP-3.]

Discussion for Automated Marking (AC-15)

Access Enforcement | Role-based Access Control (AC-3(7))

Description for Access Enforcement | Role-based Access Control (AC-3(7))
Enforce a role-based access control policy over defined subjects and objects and control access based upon [Assignment: organization-defined roles and users authorized to assume such roles].

Discussion for Access Enforcement | Role-based Access Control (AC-3(7))
Role-based access control (RBAC) is an access control policy that enforces access to objects 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) to perform needed operations on the systems associated with the organization-defined roles. When users are assigned to specific roles, they inherit the authorizations or privileges defined for those roles. RBAC simplifies privilege administration for organizations because privileges are not assigned directly to every user (which can be a large number of individuals) but are instead acquired through role assignments. RBAC can also increase privacy and security risk if individuals assigned to a role are given access to information beyond what they need to support organizational missions or business functions. RBAC can be implemented as a mandatory or discretionary form of access control. For organizations implementing RBAC with mandatory access controls, the requirements in AC-3(3) define the scope of the subjects and objects covered by the policy.

Access Enforcement | Revocation of Access Authorizations (AC-3(8))

Description for Access Enforcement | Revocation of Access Authorizations (AC-3(8))
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].

Discussion for Access Enforcement | Revocation of Access Authorizations (AC-3(8))
Revocation of access rules may differ based on the types of access revoked. 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 object is opened or the next time the subject attempts to access the object. Revocation based on changes to security labels may take effect immediately. Organizations provide alternative approaches on how to make revocations immediate if systems cannot provide such capability and immediate revocation is necessary.

Access Enforcement | Controlled Release (AC-3(9))

Description for Access Enforcement | Controlled Release (AC-3(9))
Release information outside of the system only if:
(a) The receiving [Assignment: organization-defined system or system component] provides [Assignment: organization-defined controls]; and
(b) [Assignment: organization-defined controls] are used to validate the appropriateness of the information designated for release.

Discussion for Access Enforcement | Controlled Release (AC-3(9))
Organizations can only directly protect information when it resides within the system. Additional controls may be needed to ensure that organizational information is adequately protected once it is transmitted outside of the system. In situations where the system is unable to determine the adequacy of the protections provided by external entities, as a mitigation measure, organizations procedurally determine whether the external systems are providing adequate controls. The means used to determine the adequacy of controls provided by external systems include conducting periodic assessments (inspections/tests), 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 not be the same 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 are appropriate for 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.

Access Enforcement | Audited Override of Access Control Mechanisms (AC-3(10))

Description for Access Enforcement | Audited Override of Access Control Mechanisms (AC-3(10))
Employ an audited override of automated access control mechanisms under [Assignment: organization-defined conditions] by [Assignment: organization-defined roles].

Discussion for Access Enforcement | Audited Override of Access Control Mechanisms (AC-3(10))
In certain situations, such as when there is a threat to human life or an event that threatens the organization's ability to carry out critical missions or business functions, an override capability for access control mechanisms may be needed. Override conditions are defined by organizations and used only in those limited circumstances. Audit events are defined in AU-2. Audit records are generated in AU-12.

Access Enforcement | Restrict Access to Specific Information Types (AC-3(11))

Description for Access Enforcement | Restrict Access to Specific Information Types (AC-3(11))
Restrict access to data repositories containing [Assignment: organization-defined information types].

Discussion for Access Enforcement | Restrict Access to Specific Information Types (AC-3(11))
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 to only 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 cryptographic keys, authentication information, and selected system information.

Access Enforcement | Assert and Enforce Application Access (AC-3(12))

Description for Access Enforcement | Assert and Enforce Application Access (AC-3(12))
(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];
(b) Provide an enforcement mechanism to prevent unauthorized access; and
(c) Approve access changes after initial installation of the application.

Discussion for Access Enforcement | Assert and Enforce Application Access (AC-3(12))
Asserting and enforcing application access is intended to address applications that need to access existing system applications and functions, including user contacts, global positioning systems, cameras, keyboards, microphones, networks, phones, or other files.

Access Enforcement | Attribute-based Access Control (AC-3(13))

Description for Access Enforcement | Attribute-based Access Control (AC-3(13))
Enforce attribute-based access control policy over defined subjects and objects and control access based upon [Assignment: organization-defined attributes to assume access permissions].

Discussion for Access Enforcement | Attribute-based Access Control (AC-3(13))
Attribute-based access control is an access control policy that restricts system access to authorized users based on specified organizational attributes (e.g., job function, identity), action attributes (e.g., read, write, delete), environmental attributes (e.g., time of day, location), and resource attributes (e.g., classification of a document). Organizations can create rules based on attributes and the authorizations (i.e., privileges) to perform needed operations on the systems associated with organization-defined attributes and rules. When users are assigned to attributes defined in attribute-based access control policies or rules, they can be provisioned to a system with the appropriate privileges or dynamically granted access to a protected resource. Attribute-based access control can be implemented as either a mandatory or discretionary form of access control. When implemented with mandatory access controls, the requirements in AC-3(3) define the scope of the subjects and objects covered by the policy.

Access Enforcement | Individual Access (AC-3(14))

Description for Access Enforcement | Individual Access (AC-3(14))
Provide [Assignment: organization-defined mechanisms] to enable individuals to have access to the following elements of their personally identifiable information: [Assignment: organization-defined elements].

Discussion for Access Enforcement | Individual Access (AC-3(14))
Individual access affords individuals the ability to review personally identifiable information about them held within organizational records, regardless of format. Access helps individuals to develop an understanding about how their personally identifiable information is being processed. It can also help individuals ensure that their data is accurate. Access mechanisms can include request forms and application interfaces. For federal agencies, PRIVACT processes can be located in systems of record notices and on agency websites. Access to certain types of records may not be appropriate (e.g., for federal agencies, law enforcement records within a system of records may be exempt from disclosure under the PRIVACT) or may require certain levels of authentication assurance. Organizational personnel consult with the senior agency official for privacy and legal counsel to determine appropriate mechanisms and access rights or limitations.

Access Enforcement | Discretionary and Mandatory Access Control (AC-3(15))

Description for Access Enforcement | Discretionary and Mandatory Access Control (AC-3(15))
(a) Enforce [Assignment: organization-defined mandatory access control policy] over the set of covered subjects and objects specified in the policy; and
(b) Enforce [Assignment: organization-defined discretionary access control policy] over the set of covered subjects and objects specified in the policy.

Discussion for Access Enforcement | Discretionary and Mandatory Access Control (AC-3(15))
Simultaneously implementing a mandatory access control policy and a discretionary access control policy can provide additional protection against the unauthorized execution of code by users or processes acting on behalf of users. This helps prevent a single compromised user or process from compromising the entire system.

Information Flow Enforcement (AC-4)

Description for Information Flow Enforcement (AC-4)
Enforce approved authorizations for controlling the flow of information within the system and between connected systems based on [Assignment: organization-defined information flow control policies].

Discussion for Information Flow Enforcement (AC-4)
Information flow control regulates where information can travel within a system and between systems (in contrast to who is allowed to access the information) and without regard to subsequent accesses to that information. Flow control restrictions include blocking external traffic that claims to be from within the organization, keeping export-controlled information from being transmitted in the clear to the Internet, restricting web requests that are not from the internal web proxy server, and limiting information transfers between organizations based on data structures and content. Transferring information between organizations may require an agreement specifying how the information flow is enforced (see CA-3). Transferring information between systems in different security or privacy domains with different security or privacy policies introduces the risk that such transfers violate one or more domain security or privacy policies. In such situations, information owners/stewards provide guidance at designated policy enforcement points between connected systems. Organizations consider mandating specific architectural solutions to enforce specific security and privacy policies. Enforcement includes prohibiting information transfers between connected systems (i.e., allowing access only), verifying write permissions before accepting information from another security or privacy domain or connected system, employing hardware mechanisms to enforce one-way information flows, and implementing trustworthy regrading mechanisms to reassign security or privacy attributes and labels.
Organizations commonly employ information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations within systems and between connected systems. Flow control is based on the characteristics of the information and/or the information path. Enforcement occurs, for example, in boundary protection devices that employ rule sets or establish configuration settings that restrict system services, provide a packet-filtering capability based on header information, or provide a message-filtering capability based on message content. Organizations also consider the trustworthiness of filtering and/or inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement. Control enhancements 3 through 32 primarily address cross-domain solution needs that focus on more advanced filtering techniques, in-depth analysis, and stronger flow enforcement mechanisms implemented in cross-domain products, such as high-assurance guards. Such capabilities are generally

not available in commercial off-the-shelf products. Information flow enforcement also applies to control plane traffic (e.g., routing and DNS).

Information Flow Enforcement | Object Security and Privacy Attributes (AC-4(1))

Description for Information Flow Enforcement | Object Security and Privacy Attributes (AC-4(1))
Use [Assignment: organization-defined security and privacy attributes] associated with [Assignment: organization-defined information, source, and destination objects] to enforce [Assignment: organization-defined information flow control policies] as a basis for flow control decisions.

Discussion for Information Flow Enforcement | Object Security and Privacy Attributes (AC-4(1))
Information flow enforcement mechanisms compare security and privacy attributes associated with information (i.e., data content and structure) and source and destination objects and respond appropriately when the enforcement mechanisms encounter information flows not explicitly allowed by information flow policies. For example, an information object labeled Secret would be allowed to flow to a destination object labeled Secret, but an information object labeled Top Secret would not be allowed to flow to a destination object labeled Secret. A dataset of personally identifiable information may be tagged with restrictions against combining with other types of datasets and, thus, would not be allowed to flow to the restricted dataset. Security and privacy attributes can also include source and destination addresses employed in traffic filter firewalls. Flow enforcement using explicit security or privacy attributes can be used, for example, to control the release of certain types of information.

Information Flow Enforcement | Processing Domains (AC-4(2))

Description for Information Flow Enforcement | Processing Domains (AC-4(2))
Use protected processing domains to enforce [Assignment: organization-defined information flow control policies] as a basis for flow control decisions.

Discussion for Information Flow Enforcement | Processing Domains (AC-4(2))
Protected processing domains within systems are processing spaces that have controlled interactions with other processing spaces, enabling control of information flows between these spaces and to/from information objects. A protected processing domain can be provided, for example, by implementing domain and type enforcement. In domain and type enforcement, system processes are assigned to domains, information is identified by types, and information flows are controlled based on allowed information accesses (i.e., determined by domain and type), allowed signaling among domains, and allowed process transitions to other domains.

Information Flow Enforcement | Dynamic Information Flow Control (AC-4(3))

Description for Information Flow Enforcement | Dynamic Information Flow Control (AC-4(3))
Enforce [Assignment: organization-defined information flow control policies].

Discussion for Information Flow Enforcement | Dynamic Information Flow Control (AC-4(3))
Organizational policies regarding dynamic information flow control include allowing or disallowing information flows based on changing conditions or mission or operational considerations. Changing conditions include changes in risk tolerance due to changes in the immediacy of mission or business needs, changes in the threat environment, and detection of potentially harmful or adverse events.

Information Flow Enforcement | Flow Control of Encrypted Information (AC-4(4))

Description for Information Flow Enforcement | Flow Control of Encrypted Information (AC-4(4))
Prevent encrypted information from bypassing [Assignment: organization-defined information flow control mechanisms] by [Selection (one or more): decrypting the information; blocking the flow of the encrypted information; terminating communications sessions attempting to pass encrypted information; [Assignment: organization-defined procedure or method]].

Discussion for Information Flow Enforcement | Flow Control of Encrypted Information (AC-4(4))
Flow control mechanisms include content checking, security policy filters, and data type identifiers. The term encryption is extended to cover encoded data not recognized by filtering mechanisms.

Information Flow Enforcement | Embedded Data Types (AC-4(5))

Description for Information Flow Enforcement | Embedded Data Types (AC-4(5))
Enforce [Assignment: organization-defined limitations] on embedding data types within other data types.

Discussion for Information Flow Enforcement | Embedded Data Types (AC-4(5))
Embedding data types within other data types may result in reduced flow control effectiveness. Data type embedding includes inserting files as objects within other files and using compressed or archived data types that may include multiple embedded data types. Limitations on data type embedding consider the levels of embedding and prohibit levels of data type embedding that are beyond the capability of the inspection tools.

Information Flow Enforcement | Metadata (AC-4(6))

Description for Information Flow Enforcement | Metadata (AC-4(6))
Enforce information flow control based on [Assignment: organization-defined metadata].

Discussion for Information Flow Enforcement | Metadata (AC-4(6))
Metadata is information that describes the characteristics of data. Metadata can include structural metadata describing data structures or descriptive metadata describing data content. Enforcement of allowed information flows based on metadata enables simpler and more effective flow control. Organizations consider the trustworthiness of metadata regarding data accuracy (i.e., knowledge that the metadata values are correct with respect to the data), data integrity (i.e., protecting against unauthorized changes to metadata tags), and the binding of metadata to the data payload (i.e., employing sufficiently strong binding techniques with appropriate assurance).

Information Flow Enforcement | One-way Flow Mechanisms (AC-4(7))

Description for Information Flow Enforcement | One-way Flow Mechanisms (AC-4(7))
Enforce one-way information flows through hardware-based flow control mechanisms.

Discussion for Information Flow Enforcement | One-way Flow Mechanisms (AC-4(7))
One-way flow mechanisms may also be referred to as a unidirectional network, unidirectional security gateway, or data diode. One-way flow mechanisms can be used to prevent data from being exported from a higher impact or classified domain or system while permitting data from a lower impact or unclassified domain or system to be imported.

Information Flow Enforcement | Security and Privacy Policy Filters (AC-4(8))

Description for Information Flow Enforcement | Security and Privacy Policy Filters (AC-4(8))
(a) Enforce information flow control using [Assignment: organization-defined security or privacy policy filters] as a basis for flow control decisions for [Assignment: organization-defined information flows]; and
(b) [Selection (one or more): Block; Strip; Modify; Quarantine] data after a filter processing failure in accordance with [Assignment: organization-defined security or privacy policy].

Discussion for Information Flow Enforcement | Security and Privacy Policy Filters (AC-4(8))
Organization-defined security or privacy policy filters can address data structures and content. For example, security or privacy policy filters for data structures can check for maximum file lengths, maximum field sizes, and data/file types (for structured and unstructured data). Security or privacy policy filters for data content can check for specific words, enumerated values or data value ranges, and hidden content. Structured data permits the interpretation of data content by applications. Unstructured data refers to digital information without a data structure or with a data structure that does not facilitate the development of rule sets to address the impact or classification level of the information conveyed by the data or the flow enforcement decisions. Unstructured data consists of bitmap objects that are inherently non-language-based (i.e., image, video, or audio files) and textual objects that are based on written or printed languages. Organizations can implement more than one security or privacy policy filter to meet information flow control objectives.

Information Flow Enforcement | Human Reviews (AC-4(9))

Description for Information Flow Enforcement | Human Reviews (AC-4(9))
Enforce the use of human reviews for [Assignment: organization-defined information flows] under the following conditions: [Assignment: organization-defined conditions].

Discussion for Information Flow Enforcement | Human Reviews (AC-4(9))
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 review may be employed in lieu of or as a complement to automated security or privacy policy filtering. Human reviews may also be employed as deemed necessary by organizations.

Information Flow Enforcement | Enable and Disable Security or Privacy Policy Filters (AC-4(10))

Description for Information Flow Enforcement | Enable and Disable Security or Privacy Policy Filters (AC-4(10))
Provide the capability for privileged administrators to enable and disable [Assignment: organization-defined security or privacy policy filters] under the following conditions: [Assignment: organization-defined conditions].

Discussion for Information Flow Enforcement | Enable and Disable Security or Privacy Policy Filters (AC-4(10))
For example, as allowed by the system authorization, administrators can enable security or privacy policy filters to accommodate approved data types. Administrators also have the capability to select the filters that are executed on a specific data flow based on the type of data that is being transferred, the source and destination security domains, and other security or privacy relevant features, as needed.

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

Description for Information Flow Enforcement | Configuration of Security or Privacy Policy Filters (AC-4(11))
Provide the capability for privileged administrators to configure [Assignment: organization-defined security or privacy policy filters] to support different security or privacy policies.

Discussion for Information Flow Enforcement | Configuration of Security or Privacy Policy Filters (AC-4(11))
Documentation 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 inappropriate words that security or privacy policy mechanisms check in accordance with the definitions provided by organizations.

Information Flow Enforcement | Data Type Identifiers (AC-4(12))

Description for Information Flow Enforcement | Data Type Identifiers (AC-4(12))
When transferring information between different security domains, use [Assignment: organization-defined data type identifiers] to validate data essential for information flow decisions.

Discussion for Information Flow Enforcement | Data Type Identifiers (AC-4(12))
Data type identifiers include filenames, file types, file signatures or tokens, and multiple internal file signatures or tokens. Systems only allow transfer of data that is compliant 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 used for data type identification. Content is validated syntactically and semantically against its specification to ensure that it is the proper data type.

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

Description for Information Flow Enforcement | Decomposition into Policy-relevant Subcomponents (AC-4(13))
When transferring information between different security domains, decompose information into [Assignment: organization-defined policy-relevant subcomponents] for submission to policy enforcement mechanisms.

Discussion for Information Flow Enforcement | Decomposition into Policy-relevant Subcomponents (AC-4(13))
Decomposing information into policy-relevant subcomponents prior to information transfer facilitates policy decisions on source, destination, certificates, classification, attachments, and other security- or privacy-related component differentiators. Policy enforcement mechanisms apply filtering, inspection, and/or sanitization rules to the policy-relevant subcomponents of information to facilitate flow enforcement prior to transferring such information to different security domains.

Information Flow Enforcement | Security or Privacy Policy Filter Constraints (AC-4(14))

Description for Information Flow Enforcement | Security or Privacy Policy Filter Constraints (AC-4(14))
When transferring information between different security domains, implement [Assignment: organization-defined security or privacy policy filters] requiring fully enumerated formats that restrict data structure and content.

Discussion for Information Flow Enforcement | Security or Privacy Policy Filter Constraints (AC-4(14))
Data structure and content restrictions reduce the range of potential malicious or unsanctioned content in cross-domain transactions. Security or privacy policy filters that restrict data structures include restricting file sizes and field lengths. Data content policy filters include encoding formats for character sets, restricting character data fields to only contain alpha-numeric characters, prohibiting special characters, and validating schema structures.

Information Flow Enforcement | Detection of Unsanctioned Information (AC-4(15))

Description for Information Flow Enforcement | Detection of Unsanctioned Information (AC-4(15))
When transferring information between different security domains, examine the information for the presence of [Assignment: organization-defined unsanctioned information] and prohibit the transfer of such information in accordance with the [Assignment: organization-defined security or privacy policy].

Discussion for Information Flow Enforcement | Detection of Unsanctioned Information (AC-4(15))
Unsanctioned information includes malicious code, information that is inappropriate for release from the source network, or executable code that could disrupt or harm the services or systems on the destination network.

Remote Access | Monitoring for Unauthorized Connections (AC-17(5))

Description for Remote Access | Monitoring for Unauthorized Connections (AC-17(5))
[Withdrawn: Incorporated into SI-4.]

Discussion for Remote Access | Monitoring for Unauthorized Connections (AC-17(5))

Information Flow Enforcement | Domain Authentication (AC-4(17))

Description for Information Flow Enforcement | Domain Authentication (AC-4(17))
Uniquely identify and authenticate source and destination points by [Selection (one or more): organization; system; application; service; individual] for information transfer.

Discussion for Information Flow Enforcement | Domain Authentication (AC-4(17))
Attribution is a critical component of a security and privacy concept of operations. The ability to identify source and destination points for information flowing within systems allows the forensic reconstruction of events and encourages policy compliance by attributing policy violations to specific organizations or individuals. Successful domain authentication requires that system labels distinguish among systems, organizations, and individuals involved in preparing, sending, receiving, or disseminating information. Attribution also allows organizations to better maintain the lineage of personally identifiable information processing as it flows through systems and can facilitate consent tracking, as well as correction, deletion, or access requests from individuals.

Remote Access | Additional Protection for Security Function Access (AC-17(7))

Description for Remote Access | Additional Protection for Security Function Access (AC-17(7))
[Withdrawn: Incorporated into AC-3(10).]

Discussion for Remote Access | Additional Protection for Security Function Access (AC-17(7))

Information Flow Enforcement | Validation of Metadata (AC-4(19))

Description for Information Flow Enforcement | Validation of Metadata (AC-4(19))
When transferring information between different security domains, implement [Assignment: organization-defined security or privacy policy filters] on metadata.

Discussion for Information Flow Enforcement | Validation of Metadata (AC-4(19))
All information (including metadata and the data to which the metadata applies) is subject to filtering and inspection. Some organizations distinguish between metadata and data payloads (i.e., only the data to which the metadata is bound). Other organizations do not make such distinctions and consider metadata and the data to which the metadata applies to be part of the payload.

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

Description for Information Flow Enforcement | Approved Solutions (AC-4(20))
Employ [Assignment: organization-defined solutions in approved configurations] to control the flow of [Assignment: organization-defined information] across security domains.

Discussion for Information Flow Enforcement | Approved Solutions (AC-4(20))
Organizations define approved solutions and configurations in cross-domain policies and guidance in accordance with the types of information flows across classification boundaries. The National Security Agency (NSA) National Cross Domain Strategy and Management Office provides a listing of approved cross-domain solutions. Contact ncdsmo@nsa.gov for more information.

Information Flow Enforcement | Physical or Logical Separation of Information Flows (AC-4(21))

Description for Information Flow Enforcement | Physical or Logical Separation of Information Flows (AC-4(21))
Separate information flows logically or physically using [Assignment: organization-defined mechanisms and/or techniques] to accomplish [Assignment: organization-defined required separations by types of information].

Discussion for Information Flow Enforcement | Physical or Logical Separation of Information Flows (AC-4(21))
Enforcing the separation of information flows associated with defined types of data can enhance protection by ensuring that information is not commingled while in transit and by enabling flow control by transmission paths that are not otherwise achievable. Types of separable information include inbound and outbound communications traffic, service requests and responses, and information of differing security impact or classification levels.

Information Flow Enforcement | Access Only (AC-4(22))

Description for Information Flow Enforcement | Access Only (AC-4(22))
Provide access from a single device to computing platforms, applications, or data residing in multiple different security domains, while preventing information flow between the different security domains.

Discussion for Information Flow Enforcement | Access Only (AC-4(22))
The system provides a capability for users to access each connected security domain without providing any mechanisms to allow users to transfer 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 assuredly keeping the information separate.

Information Flow Enforcement | Modify Non-releasable Information (AC-4(23))

Description for Information Flow Enforcement | Modify Non-releasable Information (AC-4(23))
When transferring information between different security domains, modify non-releasable information by implementing [Assignment: organization-defined modification action].

Discussion for Information Flow Enforcement | Modify Non-releasable Information (AC-4(23))
Modifying non-releasable information can help prevent a data spill or attack when information is transferred across security domains. Modification actions include masking, permutation, alteration, removal, or redaction.

Information Flow Enforcement | Internal Normalized Format (AC-4(24))

Description for Information Flow Enforcement | Internal Normalized Format (AC-4(24))
When transferring information between different security domains, parse incoming data into an internal normalized format and regenerate the data to be consistent with its intended specification.

Discussion for Information Flow Enforcement | Internal Normalized Format (AC-4(24))
Converting data into normalized forms is one of most of effective mechanisms to stop malicious attacks and large classes of data exfiltration.

Information Flow Enforcement | Data Sanitization (AC-4(25))

Description for Information Flow Enforcement | Data Sanitization (AC-4(25))
When transferring information between different security domains, sanitize data to minimize [Selection (one or more): delivery of malicious content, command and control of malicious code, malicious code augmentation, and steganography encoded data; spillage of sensitive information] in accordance with [Assignment: organization-defined policy]].

Discussion for Information Flow Enforcement | Data Sanitization (AC-4(25))
Data sanitization is the process of irreversibly removing or destroying data stored on a memory device (e.g., hard drives, flash memory/solid state drives, mobile devices, CDs, and DVDs) or in hard copy form.

Information Flow Enforcement | Audit Filtering Actions (AC-4(26))

Description for Information Flow Enforcement | Audit Filtering Actions (AC-4(26))
When transferring information between different security domains, record and audit content filtering actions and results for the information being filtered.

Discussion for Information Flow Enforcement | Audit Filtering Actions (AC-4(26))
Content filtering is the process of inspecting information as it traverses a cross-domain solution and determines if the information meets a predefined policy. Content filtering actions and the results of filtering actions are recorded for individual messages to ensure that the correct filter actions were applied. Content filter reports are used to assist in troubleshooting actions by, for example, determining why message content was modified and/or why it failed the filtering process. Audit events are defined in AU-2. Audit records are generated in AU-12.

Information Flow Enforcement | Redundant/independent Filtering Mechanisms (AC-4(27))

Description for Information Flow Enforcement | Redundant/independent Filtering Mechanisms (AC-4(27))
When transferring information between different security domains, implement content filtering solutions that provide redundant and independent filtering mechanisms for each data type.

Discussion for Information Flow Enforcement | Redundant/independent Filtering Mechanisms (AC-4(27))
Content filtering is the process of inspecting information as it traverses a cross-domain solution and determines if the information meets a predefined policy. Redundant and independent content filtering eliminates a single point of failure filtering system. Independence is defined as the implementation of a content filter that uses a different code base and supporting libraries (e.g., two JPEG filters using different vendors' JPEG libraries) and multiple, independent system processes.

Information Flow Enforcement | Linear Filter Pipelines (AC-4(28))

Description for Information Flow Enforcement | Linear Filter Pipelines (AC-4(28))
When transferring information between different security domains, implement a linear content filter pipeline that is enforced with discretionary and mandatory access controls.

Discussion for Information Flow Enforcement | Linear Filter Pipelines (AC-4(28))
Content filtering is the process of inspecting information as it traverses a cross-domain solution and determines if the information meets a predefined policy. The use of linear content filter pipelines ensures that filter processes are non-bypassable and always invoked. In general, the use of parallel filtering architectures for content filtering of a single data type introduces bypass and non-invocation issues.

Information Flow Enforcement | Filter Orchestration Engines (AC-4(29))

Description for Information Flow Enforcement | Filter Orchestration Engines (AC-4(29))
When transferring information between different security 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].

Discussion for Information Flow Enforcement | Filter Orchestration Engines (AC-4(29))
Content filtering is the process of inspecting information as it traverses a cross-domain solution and determines if the information meets a predefined security policy. An orchestration engine coordinates the sequencing of activities (manual and automated) in a content filtering process. Errors are defined as either anomalous actions or unexpected termination of the content filter process. This is not the same as a filter failing content due to non-compliance with policy. Content filter reports are a commonly used mechanism to ensure that expected filtering actions are completed successfully.

Information Flow Enforcement | Filter Mechanisms Using Multiple Processes (AC-4(30))

Description for Information Flow Enforcement | Filter Mechanisms Using Multiple Processes (AC-4(30))
When transferring information between different security domains, implement content filtering mechanisms using multiple processes.

Discussion for Information Flow Enforcement | Filter Mechanisms Using Multiple Processes (AC-4(30))
The use of multiple processes to implement content filtering mechanisms reduces the likelihood of a single point of failure.

Information Flow Enforcement | Failed Content Transfer Prevention (AC-4(31))

Description for Information Flow Enforcement | Failed Content Transfer Prevention (AC-4(31))
When transferring information between different security domains, prevent the transfer of failed content to the receiving domain.

Discussion for Information Flow Enforcement | Failed Content Transfer Prevention (AC-4(31))
Content that failed filtering checks can corrupt the system if transferred to the receiving domain.

Information Flow Enforcement | Process Requirements for Information Transfer (AC-4(32))

Description for Information Flow Enforcement | Process Requirements for Information Transfer (AC-4(32))
When transferring information between different security domains, the process that transfers information between filter pipelines:
(a) Does not filter message content;
(b) Validates filtering metadata;
(c) Ensures the content associated with the filtering metadata has successfully completed filtering; and
(d) Transfers the content to the destination filter pipeline.

Discussion for Information Flow Enforcement | Process Requirements for Information Transfer (AC-4(32))
The processes transferring information between filter pipelines have minimum complexity and functionality to provide assurance that the processes operate correctly.

Separation of Duties (AC-5)

Description for Separation of Duties (AC-5)
a. Identify and document [Assignment: organization-defined duties of individuals requiring separation]; and
b. Define system access authorizations to support separation of duties.

Discussion for Separation of Duties (AC-5)
Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes dividing mission or business functions and support functions among different individuals or roles, conducting system support functions with different individuals, and ensuring that security personnel who administer access

control functions do not also administer audit functions. Because separation of duty violations can span systems and application domains, organizations consider the entirety of systems and system components when developing policy on separation of duties. Separation of duties is enforced through the account management activities in AC-2, access control mechanisms in AC-3, and identity management activities in IA-2, IA-4, and IA-12.

Least Privilege (AC-6)

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

Discussion for Least Privilege (AC-6)
Organizations employ least privilege for specific duties and systems. The principle of least privilege is also applied to system processes, ensuring that the processes have access to systems and operate at privilege levels no higher than necessary to accomplish organizational missions 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.

Least Privilege | Authorize Access to Security Functions (AC-6(1))

Description for Least Privilege | Authorize Access to Security Functions (AC-6(1))
Authorize access for [Assignment: organization-defined individuals or roles] to:
(a) [Assignment: organization-defined security functions (deployed in hardware, software, and firmware)]; and
(b) [Assignment: organization-defined security-relevant information].

Discussion for Least Privilege | Authorize Access to Security Functions (AC-6(1))
Security functions include establishing system accounts, configuring access authorizations (i.e., permissions, privileges), configuring settings for events to be audited, and establishing intrusion detection parameters. Security-relevant information includes filtering rules for routers or firewalls, configuration parameters for security services, cryptographic key management information, and access control lists. Authorized personnel include security administrators, system administrators, system security officers, system programmers, and other privileged users.

Least Privilege | Non-privileged Access for Nonsecurity Functions (AC-6(2))

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

Discussion for Least Privilege | Non-privileged Access for Nonsecurity Functions (AC-6(2))
Requiring the use of non-privileged accounts when accessing nonsecurity functions limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses 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 the user and the processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account.

Least Privilege | Network Access to Privileged Commands (AC-6(3))

Description for Least Privilege | Network Access to Privileged Commands (AC-6(3))
Authorize network access to [Assignment: organization-defined privileged commands] only for [Assignment: organization-defined compelling operational needs] and document the rationale for such access in the security plan for the system.

Discussion for Least Privilege | Network Access to Privileged Commands (AC-6(3))
Network access is any access across a network connection in lieu of local access (i.e., user being physically present at the device).

Least Privilege | Separate Processing Domains (AC-6(4))

Description for Least Privilege | Separate Processing Domains (AC-6(4))
Provide separate processing domains to enable finer-grained allocation of user privileges.

Discussion for Least Privilege | Separate Processing Domains (AC-6(4))
Providing separate processing domains for finer-grained allocation of user privileges includes using virtualization 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.

Least Privilege | Privileged Accounts (AC-6(5))

Description for Least Privilege | Privileged Accounts (AC-6(5))
Restrict privileged accounts on the system to [Assignment: organization-defined personnel or roles].

Discussion for Least Privilege | Privileged Accounts (AC-6(5))
Privileged accounts, including super user accounts, are typically described as system administrator for various types of commercial off-the-shelf operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from accessing privileged information or privileged functions. Organizations may differentiate in the application of restricting privileged accounts between allowed privileges for local accounts and for domain accounts provided that they retain the ability to control system configurations for key parameters and as otherwise necessary to sufficiently mitigate risk.

Least Privilege | Privileged Access by Non-organizational Users (AC-6(6))

Description for Least Privilege | Privileged Access by Non-organizational Users (AC-6(6))
Prohibit privileged access to the system by non-organizational users.

Discussion for Least Privilege | Privileged Access by Non-organizational Users (AC-6(6))
An organizational user is an employee or an individual considered by the organization to have the equivalent status of an employee. Organizational users include contractors, guest researchers, or individuals detailed from other organizations. A non-organizational user is a user who is not an organizational user. Policies and procedures for granting equivalent status of employees to individuals include a need-to-know, citizenship, and the relationship to the organization.

Least Privilege | Review of User Privileges (AC-6(7))

Description for Least Privilege | Review of User Privileges (AC-6(7))
(a) Review [Assignment: organization-defined frequency] the privileges assigned to [Assignment: organization-defined roles or classes of users] to validate the need for such privileges; and
(b) Reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs.

Discussion for Least Privilege | Review of User Privileges (AC-6(7))
The need for certain assigned user privileges may change over time to reflect changes in organizational mission and business functions, environments of operation, technologies, or threats. A periodic review of assigned user privileges is necessary to determine if the rationale for assigning such privileges remains valid. If the need cannot be revalidated, organizations take appropriate corrective actions.

Least Privilege | Privilege Levels for Code Execution (AC-6(8))

Description for Least Privilege | Privilege Levels for Code Execution (AC-6(8))
Prevent the following software from executing at higher privilege levels than users executing the software: [Assignment: organization-defined software].

Discussion for Least Privilege | Privilege Levels for Code Execution (AC-6(8))
In certain situations, software applications or programs need to execute with elevated privileges to perform required functions. However, depending on the software functionality and configuration, if the privileges required for execution are at a higher level than the privileges assigned to organizational users invoking such applications or programs, those users may indirectly be provided with greater privileges than assigned.

Least Privilege | Log Use of Privileged Functions (AC-6(9))

Description for Least Privilege | Log Use of Privileged Functions (AC-6(9))
Log the execution of privileged functions.

Discussion for Least Privilege | Log Use of Privileged Functions (AC-6(9))
The misuse of privileged functions, either intentionally or unintentionally by authorized users or by unauthorized external entities that have compromised system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Logging and analyzing the use of privileged functions is one way to detect such misuse and, in doing so, help mitigate the risk from insider threats and the advanced persistent threat.

Least Privilege | Prohibit Non-privileged Users from Executing Privileged Functions (AC-6(10))

Description for Least Privilege | Prohibit Non-privileged Users from Executing Privileged Functions (AC-6(10))
Prevent non-privileged users from executing privileged functions.

Discussion for Least Privilege | Prohibit Non-privileged Users from Executing Privileged Functions (AC-6(10))
Privileged functions include disabling, circumventing, or altering implemented security or privacy controls, establishing system accounts, performing system integrity checks, and administering cryptographic key management activities. Non-privileged users are individuals who do not possess appropriate authorizations. Privileged functions that require protection from non-privileged users include circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms. Preventing non-privileged users from executing privileged functions is enforced by AC-3.

Unsuccessful Logon Attempts (AC-7)

Description for Unsuccessful Logon Attempts (AC-7)
a. Enforce a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period]; and
b. Automatically [Selection (one or more): lock the account or node for an [Assignment: organization-defined time period]; lock the account or node until released by an administrator; delay next logon prompt per [Assignment: organization-defined delay algorithm]; notify system administrator; take other [Assignment: organization-defined action]] when the maximum number of unsuccessful attempts is exceeded.

Discussion for Unsuccessful Logon Attempts (AC-7)
The need to limit unsuccessful logon attempts and take subsequent action when the maximum number of attempts is exceeded applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by systems are usually temporary and automatically release after a predetermined, organization-defined time period. If a delay algorithm is selected, organizations may employ different algorithms for different components of the system based on the capabilities of those components. Responses to unsuccessful logon attempts may be implemented at the operating system and the application levels. Organization-defined actions that may be taken when the number of allowed consecutive invalid logon attempts is exceeded include prompting the user to answer a secret question in addition to the username and password, invoking a lockdown mode with limited user capabilities (instead of full lockout), allowing users to only logon from specified Internet Protocol (IP) addresses, requiring a CAPTCHA to prevent automated attacks, or applying user profiles such as location, time of day, IP address, device, or Media Access Control (MAC) address. If automatic system lockout or execution of a delay algorithm is not implemented in support of the availability objective, organizations consider a combination of other actions to help prevent brute force attacks. In addition to the above, organizations can prompt users to respond to a secret question before the number of allowed unsuccessful logon attempts is exceeded. Automatically unlocking an account after a specified period of time is generally not permitted. However, exceptions may be required based on operational mission or need.

Remote Access | Disable Nonsecure Network Protocols (AC-17(8))

Description for Remote Access | Disable Nonsecure Network Protocols (AC-17(8))
[Withdrawn: Incorporated into CM-7.]

Discussion for Remote Access | Disable Nonsecure Network Protocols (AC-17(8))

Unsuccessful Logon Attempts | Purge or Wipe Mobile Device (AC-7(2))

Description for Unsuccessful Logon Attempts | Purge or Wipe Mobile Device (AC-7(2))
Purge or wipe information from [Assignment: organization-defined mobile devices] based on [Assignment: organization-defined purging or wiping requirements and techniques] after [Assignment: organization-defined number] consecutive, unsuccessful device logon attempts.

Discussion for Unsuccessful Logon Attempts | Purge or Wipe Mobile Device (AC-7(2))
A mobile device is a computing device that has a small form factor such that it can be carried by a single individual; is designed to operate without a physical connection; possesses local, non-removable or removable data storage; and includes a self-contained power source. Purging or wiping the device applies only to mobile devices for which the organization-defined number of unsuccessful logons occurs. The logon is to the mobile device, not to any one account on the

device. Successful logons to accounts on mobile devices reset the unsuccessful logon count to zero. Purging or wiping may be unnecessary if the information on the device is protected with sufficiently strong encryption mechanisms.

Unsuccessful Logon Attempts | Biometric Attempt Limiting (AC-7(3))

Description for Unsuccessful Logon Attempts | Biometric Attempt Limiting (AC-7(3))
Limit the number of unsuccessful biometric logon attempts to [Assignment: organization-defined number].

Discussion for Unsuccessful Logon Attempts | Biometric Attempt Limiting (AC-7(3))
Biometrics are probabilistic in nature. The ability to successfully authenticate can be impacted by many factors, including matching performance and presentation attack detection mechanisms. Organizations select the appropriate number of attempts for users based on organizationally-defined factors.

Unsuccessful Logon Attempts | Use of Alternate Authentication Factor (AC-7(4))

Description for Unsuccessful Logon Attempts | Use of Alternate Authentication Factor (AC-7(4))
(a) Allow the use of [Assignment: organization-defined authentication factors] that are different from the primary authentication factors after the number of organization-defined consecutive invalid logon attempts have been exceeded; and
(b) Enforce a limit of [Assignment: organization-defined number] consecutive invalid logon attempts through use of the alternative factors by a user during a [Assignment: organization-defined time period].

Discussion for Unsuccessful Logon Attempts | Use of Alternate Authentication Factor (AC-7(4))
The use of alternate authentication factors supports the objective of availability and allows a user who has inadvertently been locked out to use additional authentication factors to bypass the lockout.

System Use Notification (AC-8)

Description for System Use Notification (AC-8)
a. Display [Assignment: organization-defined system use notification message or banner] to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and state that:
1. Users are accessing a U.S. Government system;
2. System usage may be monitored, recorded, and subject to audit;
3. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and
4. Use of the system indicates consent to monitoring and recording;
b. Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system; and
c. 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.

Discussion for System Use Notification (AC-8)
System use notifications can be implemented using messages or warning banners displayed before individuals log in to systems. System use notifications are used only for access via logon 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 logon. Organizations consider system use notification messages or banners displayed in multiple languages based on organizational needs and the demographics of system users. Organizations consult with the privacy office for input regarding privacy messaging and the Office of the General Counsel or organizational equivalent for legal review and approval of warning banner content.

Previous Logon Notification (AC-9)

Description for Previous Logon Notification (AC-9)
Notify the user, upon successful logon to the system, of the date and time of the last logon.

Discussion for Previous Logon Notification (AC-9)
Previous logon 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 logon allows the user to recognize if the date and time provided is not consistent with the user's last access.

Previous Logon Notification | Unsuccessful Logons (AC-9(1))

Description for Previous Logon Notification | Unsuccessful Logons (AC-9(1))
Notify the user, upon successful logon, of the number of unsuccessful logon attempts since the last successful logon.

Discussion for Previous Logon Notification | Unsuccessful Logons (AC-9(1))
Information about the number of unsuccessful logon attempts since the last successful logon allows the user to recognize if the number of unsuccessful logon attempts is consistent with the user's actual logon attempts.

Previous Logon Notification | Successful and Unsuccessful Logons (AC-9(2))

Description for Previous Logon Notification | Successful and Unsuccessful Logons (AC-9(2))
Notify the user, upon successful logon, of the number of [Selection: successful logons; unsuccessful logon attempts; both] during [Assignment: organization-defined time period].

Discussion for Previous Logon Notification | Successful and Unsuccessful Logons (AC-9(2))
Information about the number of successful and unsuccessful logon attempts within a specified time period allows the user to recognize if the number and type of logon attempts are consistent with the user's actual logon attempts.

Previous Logon Notification | Notification of Account Changes (AC-9(3))

Description for Previous Logon Notification | Notification of Account Changes (AC-9(3))
Notify the user, upon successful logon, of changes to [Assignment: organization-defined security-related characteristics or parameters of the user's account] during [Assignment: organization-defined time period].

Discussion for Previous Logon Notification | Notification of Account Changes (AC-9(3))
Information about changes to security-related account characteristics within a specified time period allows users to recognize if changes were made without their knowledge.

Previous Logon Notification | Additional Logon Information (AC-9(4))

Description for Previous Logon Notification | Additional Logon Information (AC-9(4))
Notify the user, upon successful logon, of the following additional information: [Assignment: organization-defined additional information].

Discussion for Previous Logon Notification | Additional Logon Information (AC-9(4))
Organizations can specify additional information to be provided to users upon logon, including the location of the last logon. User location is defined as information that can be determined by systems, such as Internet Protocol (IP) addresses from which network logons occurred, notifications of local logons, or device identifiers.

Concurrent Session Control (AC-10)

Description for Concurrent Session Control (AC-10)
Limit the number of concurrent sessions for each [Assignment: organization-defined account and/or account type] to [Assignment: organization-defined number].

Discussion for Concurrent Session Control (AC-10)
Organizations may define the maximum number of concurrent sessions for system accounts globally, by account type, by account, or any combination thereof. For example, organizations may limit the number of concurrent sessions for system administrators or other individuals working in particularly sensitive domains or mission-critical applications. Concurrent session control addresses concurrent sessions for system accounts. It does not, however, address concurrent sessions by single users via multiple system accounts.

Device Lock (AC-11)

Description for Device Lock (AC-11)
a. Prevent further access to the system by [Selection (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
b. Retain the device lock until the user reestablishes access using established identification and authentication procedures.

Discussion for Device Lock (AC-11)
Device locks are temporary actions taken to prevent logical access to organizational systems when users stop work 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 out of systems, such as when organizations require users to log out at the end of workdays.

Device Lock | Pattern-hiding Displays (AC-11(1))

Description for Device Lock | Pattern-hiding Displays (AC-11(1))
Conceal, via the device lock, information previously visible on the display with a publicly viewable image.

Discussion for Device Lock | Pattern-hiding Displays (AC-11(1))
The pattern-hiding display can include static or dynamic images, such as patterns used with screen savers, photographic images, solid colors, clock, battery life indicator, or a blank screen with the caveat that controlled unclassified information is not displayed.

Session Termination (AC-12)

Description for Session Termination (AC-12)
Automatically terminate a user session after [Assignment: organization-defined conditions or trigger events requiring session disconnect].

Discussion for Session Termination (AC-12)
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 disconnect)). A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organizational system. Such user sessions can be terminated without terminating network sessions. Session termination ends all processes associated with a user's logical session except for those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated. Conditions or trigger events that require automatic termination of the session include organization-defined periods of user inactivity, targeted responses to certain types of incidents, or time-of-day restrictions on system use.

Session Termination | User-initiated Logouts (AC-12(1))

Description for Session Termination | User-initiated Logouts (AC-12(1))
Provide a logout capability for user-initiated communications sessions whenever authentication is used to gain access to [Assignment: organization-defined information resources].

Discussion for Session Termination | User-initiated Logouts (AC-12(1))
Information resources to which users gain access via authentication include local workstations, databases, and password-protected websites or web-based services.

Session Termination | Termination Message (AC-12(2))

Description for Session Termination | Termination Message (AC-12(2))
Display an explicit logout message to users indicating the termination of authenticated communications sessions.

Discussion for Session Termination | Termination Message (AC-12(2))
Logout messages for web access can be displayed after authenticated sessions have been terminated. However, for certain types of sessions, including file transfer protocol (FTP) sessions, systems typically send logout messages as final messages prior to terminating sessions.

Session Termination | Timeout Warning Message (AC-12(3))

Description for Session Termination | Timeout Warning Message (AC-12(3))
Display an explicit message to users indicating that the session will end in [Assignment: organization-defined time until end of session].

Discussion for Session Termination | Timeout Warning Message (AC-12(3))
To increase usability, notify users of pending session termination and prompt users to continue the session. The pending session termination time period is based on the parameters defined in the AC-12 base control.

Wireless Access | Monitoring Unauthorized Connections (AC-18(2))

Description for Wireless Access | Monitoring Unauthorized Connections (AC-18(2))
[Withdrawn: Incorporated into SI-4.]

Discussion for Wireless Access | Monitoring Unauthorized Connections (AC-18(2))

Permitted Actions Without Identification or Authentication (AC-14)

Description for Permitted Actions Without Identification or Authentication (AC-14)
a. Identify [Assignment: organization-defined user actions] that can be performed on the system without identification or authentication consistent with organizational mission and business functions; and
b. Document and provide supporting rationale in the security plan for the system, user actions not requiring identification or authentication.

Discussion for Permitted Actions Without Identification or Authentication (AC-14)
Specific user actions may be permitted without identification or authentication if organizations determine that identification and authentication are 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 publicly accessible federal systems, when individuals 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 logon functionality and is protected from accidental or unmonitored use. Permitting actions without identification or

authentication does not apply to situations where identification and authentication have already occurred and are not repeated but rather to situations where identification and authentication have not yet occurred. Organizations may decide that there are no user actions that can be performed on organizational systems without identification and authentication, and therefore, the value for the assignment operation can be none.

Access Control for Mobile Devices | Use of Writable and Portable Storage Devices (AC-19(1))

Description for Access Control for Mobile Devices | Use of Writable and Portable Storage Devices (AC-19(1))
[Withdrawn: Incorporated into MP-7.]

Discussion for Access Control for Mobile Devices | Use of Writable and Portable Storage Devices (AC-19(1))

Access Control for Mobile Devices | Use of Personally Owned Portable Storage Devices (AC-19(2))

Description for Access Control for Mobile Devices | Use of Personally Owned Portable Storage Devices (AC-19(2))
[Withdrawn: Incorporated into MP-7.]

Discussion for Access Control for Mobile Devices | Use of Personally Owned Portable Storage Devices (AC-19(2))

Security and Privacy Attributes (AC-16)

Description for Security and Privacy Attributes (AC-16)
a. Provide the means to associate [Assignment: organization-defined types of security and privacy attributes] with [Assignment: organization-defined security and privacy attribute values] for information in storage, in process, and/or in transmission;
b. Ensure that the attribute associations are made and retained with the information;
c. Establish the following permitted security and privacy attributes from the attributes defined in AC-16a for [Assignment: organization-defined systems]: [Assignment: organization-defined security and privacy attributes];
d. Determine the following permitted attribute values or ranges for each of the established attributes: [Assignment: organization-defined attribute values or ranges for established attributes];
e. Audit changes to attributes; and
f. Review [Assignment: organization-defined security and privacy attributes] for applicability [Assignment: organization-defined frequency].

Discussion for Security and Privacy Attributes (AC-16)
Information is represented internally within systems using abstractions known as data structures. Internal data structures can represent different types of entities, both active and passive. Active entities, also known as subjects, are typically associated with individuals, devices, or processes acting on behalf of individuals. Passive entities, also known as objects, are typically associated with data structures, such as records, buffers, tables, files, inter-process pipes, and communications ports. Security attributes, a form of metadata, are abstractions that represent the basic properties or characteristics of active and passive entities with respect to safeguarding information. Privacy attributes, which may be used independently or in conjunction with security attributes, represent the basic properties or characteristics of active or passive entities with respect to the management of personally identifiable information. Attributes can be either explicitly or implicitly associated with the information contained in organizational systems or system components.
Attributes may be associated with active entities (i.e., subjects) that have the

potential to send or receive information, cause information to flow among objects, or change the system state. These attributes may also be associated with passive entities (i.e., objects) that contain or receive information. The association of attributes to subjects and objects by a system is referred to as binding and is inclusive of setting the attribute value and the attribute type. Attributes, when bound to data or information, permit the enforcement of security and privacy policies for access control and information flow control, including data retention limits, permitted uses of personally identifiable information, and identification of personal information within data objects. Such enforcement occurs through organizational processes or system functions or mechanisms. The binding techniques implemented by systems affect the strength of attribute binding to information. Binding strength and the assurance associated with binding techniques play important parts in the trust that organizations have in the information flow enforcement process. The binding techniques affect the number and degree of additional reviews required by organizations. The content or assigned values of attributes can directly affect the ability of individuals to access organizational information.

Organizations can define the types of attributes needed for systems to support missions or business functions. There are many values that can be assigned to a security attribute. By specifying the permitted attribute ranges and values, organizations ensure that attribute values are meaningful and relevant. Labeling refers to the association of attributes with the subjects and objects represented by the internal data structures within systems. This facilitates system-based enforcement of information security and privacy policies. Labels include classification of information in accordance with legal and compliance requirements (e.g., top secret, secret, confidential, controlled unclassified), information impact level; high value asset information, access authorizations, nationality; data life cycle protection (i.e., encryption and data expiration), personally identifiable information processing permissions, including individual consent to personally identifiable information processing, and contractor affiliation. A related term to labeling is marking. Marking refers to the association of attributes with objects in a human-readable form and displayed on system media. Marking enables manual, procedural, or process-based enforcement of information security and privacy policies. Security and privacy labels may have the same value as media markings (e.g., top secret, secret, confidential). See MP-3 (Media Marking).

Security and Privacy Attributes | Dynamic Attribute Association (AC-16(1))

Description for Security and Privacy Attributes | Dynamic Attribute Association (AC-16(1))
Dynamically associate security and privacy attributes with [Assignment: organization-defined subjects and objects] in accordance with the following security and privacy policies as information is created and combined: [Assignment: organization-defined security and privacy policies].

Discussion for Security and Privacy Attributes | Dynamic Attribute Association (AC-16(1))
Dynamic association of attributes is appropriate whenever the security or privacy characteristics of information change over time. Attributes may change due to information aggregation issues (i.e., characteristics of individual data elements are different from the combined elements), changes in individual access authorizations (i.e., privileges), changes in the security category of information, or changes in security or privacy policies. Attributes may also change situationally.

Security and Privacy Attributes | Attribute Value Changes by Authorized Individuals (AC-16(2))

Description for Security and Privacy Attributes | Attribute Value Changes by Authorized Individuals (AC-16(2))
Provide authorized individuals (or processes acting on behalf of individuals) the capability to define or change the value of associated security and privacy attributes.

Discussion for Security and Privacy Attributes | Attribute Value Changes by Authorized Individuals (AC-16(2))
The content or assigned values of attributes can directly affect the ability of individuals to access organizational information. Therefore, it is important for systems to be able to limit the ability to create or modify attributes to authorized individuals.

Security and Privacy Attributes | Maintenance of Attribute Associations by System (AC-16(3))

Description for Security and Privacy Attributes | Maintenance of Attribute Associations by System (AC-16(3))
Maintain the association and integrity of [Assignment: organization-defined security and privacy attributes] to [Assignment: organization-defined subjects and objects].

Discussion for Security and Privacy Attributes | Maintenance of Attribute Associations by System (AC-16(3))
Maintaining the association and integrity of security and privacy attributes to subjects and objects with sufficient assurance helps to ensure that the attribute associations can be used as the basis of automated policy actions. The integrity of specific items, such as security configuration files, may be maintained through the use of an integrity monitoring mechanism that detects anomalies and changes that deviate from known good baselines. Automated policy actions include retention date expirations, access control decisions, information flow control decisions, and information disclosure decisions.

Security and Privacy Attributes | Association of Attributes by Authorized Individuals (AC-16(4))

Description for Security and Privacy Attributes | Association of Attributes by Authorized Individuals (AC-16(4))
Provide the capability to associate [Assignment: organization-defined security and privacy attributes] with [Assignment: organization-defined subjects and objects] by authorized individuals (or processes acting on behalf of individuals).

Discussion for Security and Privacy Attributes | Association of Attributes by Authorized Individuals (AC-16(4))
Systems, in general, provide the capability for privileged users to assign security and privacy attributes to system-defined subjects (e.g., users) and objects (e.g., directories, files, and ports). Some systems provide additional capability for general users to assign security and privacy attributes to additional objects (e.g., files, emails). The association of attributes by authorized individuals is described in the design documentation. The support provided by systems can include prompting users to select security and privacy attributes to be associated with information objects, employing automated mechanisms to categorize information with attributes based on defined policies, or ensuring that the combination of the security or privacy attributes selected is valid. Organizations consider the creation, deletion, or modification of attributes when defining auditable events.

Security and Privacy Attributes | Attribute Displays on Objects to Be Output (AC-16(5))

Description for Security and Privacy Attributes | Attribute Displays on Objects to Be Output (AC-16(5))
Display security and privacy attributes in human-readable form on each object that the system transmits to output devices to identify [Assignment: organization-defined special dissemination, handling, or distribution instructions] using [Assignment: organization-defined human-readable, standard naming conventions].

Discussion for Security and Privacy Attributes | Attribute Displays on Objects to Be Output (AC-16(5))
System outputs include printed pages, screens, or equivalent items. System output devices include printers, notebook computers, video displays, smart phones, and tablets. To mitigate the risk of unauthorized exposure of information (e.g., shoulder surfing), the outputs display full attribute values when unmasked by the subscriber.

Security and Privacy Attributes | Maintenance of Attribute Association (AC-16(6))

Description for Security and Privacy Attributes | Maintenance of Attribute Association (AC-16(6))
Require personnel to associate and maintain the association of [Assignment: organization-defined security and privacy attributes] with [Assignment: organization-defined subjects and objects] in accordance with [Assignment: organization-defined security and privacy policies].

Discussion for Security and Privacy Attributes | Maintenance of Attribute Association (AC-16(6))
Maintaining attribute association requires individual users (as opposed to the system) to maintain associations of defined security and privacy attributes with subjects and objects.

Security and Privacy Attributes | Consistent Attribute Interpretation (AC-16(7))

Description for Security and Privacy Attributes | Consistent Attribute Interpretation (AC-16(7))
Provide a consistent interpretation of security and privacy attributes transmitted between distributed system components.

Discussion for Security and Privacy Attributes | Consistent Attribute Interpretation (AC-16(7))
To enforce security and privacy policies across multiple system components in distributed systems, organizations provide a consistent interpretation of security and privacy attributes employed in access enforcement and flow enforcement decisions. Organizations can establish agreements and processes to help ensure that distributed system components implement attributes with consistent interpretations in automated access enforcement and flow enforcement actions.

Security and Privacy Attributes | Association Techniques and Technologies (AC-16(8))

Description for Security and Privacy Attributes | Association Techniques and Technologies (AC-16(8))
Implement [Assignment: organization-defined techniques and technologies] in associating security and privacy attributes to information.

Discussion for Security and Privacy Attributes | Association Techniques and Technologies (AC-16(8))
The association of security and privacy attributes to information within systems is important for conducting automated access enforcement and flow enforcement actions. The association of such attributes to information (i.e., binding) can be accomplished with technologies and techniques that provide different levels of assurance. For example, systems can cryptographically bind attributes to information using digital signatures that support cryptographic keys protected by hardware devices (sometimes known as hardware roots of trust).

Security and Privacy Attributes | Attribute Reassignment — Regrading Mechanisms (AC-16(9))

Description for Security and Privacy Attributes | Attribute Reassignment — Regrading Mechanisms (AC-16(9))
Change security and privacy attributes associated with information only via regrading mechanisms validated using [Assignment: organization-defined techniques or procedures].

Discussion for Security and Privacy Attributes | Attribute Reassignment — Regrading Mechanisms (AC-16(9))
A regrading mechanism is a trusted process authorized to re-classify and re-label data in accordance with a defined policy exception. Validated regrading mechanisms are used by organizations to provide the requisite levels of assurance for attribute reassignment activities. The validation is facilitated by ensuring that regrading mechanisms are single purpose and of limited function. Since security and privacy attribute changes can directly affect policy enforcement actions, implementing trustworthy regrading mechanisms is necessary to help ensure that such mechanisms perform in a consistent and correct mode of operation.

Security and Privacy Attributes | Attribute Configuration by Authorized Individuals (AC-16(10))

Description for Security and Privacy Attributes | Attribute Configuration by Authorized Individuals (AC-16(10))
Provide authorized individuals the capability to define or change the type and value of security and privacy attributes available for association with subjects and objects.

Discussion for Security and Privacy Attributes | Attribute Configuration by Authorized Individuals (AC-16(10))
The content or assigned values of security and privacy attributes can directly affect the ability of individuals to access organizational information. Thus, it is important for systems to be able to limit the ability to create or modify the type and value of attributes available for association with subjects and objects to authorized individuals only.

Remote Access (AC-17)

Description for Remote Access (AC-17)
a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and
b. Authorize each type of remote access to the system prior to allowing such connections.

Discussion for Remote Access (AC-17)
Remote access is access to organizational systems (or processes acting on behalf of users) that communicate through external networks such as the Internet. Types of remote access include dial-up, broadband, and wireless. Organizations use encrypted virtual private networks (VPNs) to enhance confidentiality and integrity for remote connections. The use of encrypted VPNs provides sufficient assurance to the organization that it can effectively treat such connections as internal networks if the cryptographic mechanisms used are implemented in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Still, VPN connections traverse external networks, and the encrypted VPN does not enhance the availability of remote connections. VPNs with encrypted tunnels can also affect the ability 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. Authorization of each remote access type addresses authorization prior to allowing remote access without specifying the specific formats for such authorization. While organizations may use information exchange and system connection security agreements to manage remote access connections to other systems, such agreements are addressed as part of CA-3. Enforcing access restrictions for remote access is addressed via AC-3.

Remote Access | Monitoring and Control (AC-17(1))

Description for Remote Access | Monitoring and Control (AC-17(1))
Employ automated mechanisms to monitor and control remote access methods.

Discussion for Remote Access | Monitoring and Control (AC-17(1))
Monitoring and control of remote access methods allows organizations to detect attacks and help ensure compliance with remote access policies by auditing the connection activities of remote users on a variety of system components, including servers, notebook computers, workstations, smart phones, and tablets. Audit logging for remote access is enforced by AU-2. Audit events are defined in AU-2a.

Remote Access | Protection of Confidentiality and Integrity Using Encryption (AC-17(2))

Description for Remote Access | Protection of Confidentiality and Integrity Using Encryption (AC-17(2))
Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

Discussion for Remote Access | Protection of Confidentiality and Integrity Using Encryption (AC-17(2))
Virtual private networks can be used to protect the confidentiality and integrity of remote access sessions. Transport Layer Security (TLS) is an example of a cryptographic protocol that provides end-to-end communications security over networks and is used for Internet communications and online transactions.

Remote Access | Managed Access Control Points (AC-17(3))

Description for Remote Access | Managed Access Control Points (AC-17(3))
Route remote accesses through authorized and managed network access control points.

Discussion for Remote Access | Managed Access Control Points (AC-17(3))
Organizations consider the Trusted Internet Connections (TIC) initiative DHS TIC requirements for external network connections since limiting the number of access control points for remote access reduces attack surfaces.

Remote Access | Privileged Commands and Access (AC-17(4))

Description for Remote Access | Privileged Commands and Access (AC-17(4))
(a) Authorize the execution of privileged commands and access to security-relevant information via remote access only in a format that provides assessable evidence and for the following needs: [Assignment: organization-defined needs]; and
(b) Document the rationale for remote access in the security plan for the system.

Discussion for Remote Access | Privileged Commands and Access (AC-17(4))
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.

Access Control for Mobile Devices | Use of Portable Storage Devices with No Identifiable Owner (AC-19(3))

Description for Access Control for Mobile Devices | Use of Portable Storage Devices with No Identifiable Owner (AC-19(3))
[Withdrawn: Incorporated into MP-7.]

Discussion for Access Control for Mobile Devices | Use of Portable Storage Devices with No Identifiable Owner (AC-19(3))

Remote Access | Protection of Mechanism Information (AC-17(6))

Description for Remote Access | Protection of Mechanism Information (AC-17(6))
Protect information about remote access mechanisms from unauthorized use and disclosure.

Discussion for Remote Access | Protection of Mechanism Information (AC-17(6))
Remote access to organizational information by non-organizational entities can increase the risk of unauthorized use and disclosure about remote access mechanisms. The organization considers including remote access requirements in the information exchange agreements with other organizations, as applicable. Remote access requirements can also be included in rules of behavior (see PL-4) and access agreements (see PS-6).

Account Management | Shared and Group Account Credential Change (AC-2(10))

Description for Account Management | Shared and Group Account Credential Change (AC-2(10))
[Withdrawn: Incorporated into AC-2k.]

Discussion for Account Management | Shared and Group Account Credential Change (AC-2(10))

Access Enforcement | Restricted Access to Privileged Functions (AC-3(1))

Description for Access Enforcement | Restricted Access to Privileged Functions (AC-3(1))
[Withdrawn: Incorporated into AC-6.]

Discussion for Access Enforcement | Restricted Access to Privileged Functions (AC-3(1))

Remote Access | Disconnect or Disable Access (AC-17(9))

Description for Remote Access | Disconnect or Disable Access (AC-17(9))
Provide the capability to disconnect or disable remote access to the system within [Assignment: organization-defined time period].

Discussion for Remote Access | Disconnect or Disable Access (AC-17(9))
The speed of system disconnect or disablement varies based on the criticality of missions or business functions and the need to eliminate immediate or future remote access to systems.

Remote Access | Authenticate Remote Commands (AC-17(10))

Description for Remote Access | Authenticate Remote Commands (AC-17(10))
Implement [Assignment: organization-defined mechanisms] to authenticate [Assignment: organization-defined remote commands].

Discussion for Remote Access | Authenticate Remote Commands (AC-17(10))
Authenticating remote commands protects against unauthorized commands and the replay of authorized commands. The ability to authenticate remote commands is important for remote systems for which loss, malfunction, misdirection, or exploitation would have immediate or serious consequences, such as injury, death, property damage, loss of high value assets, failure of mission or business functions, or compromise of classified or controlled unclassified information. Authentication mechanisms for remote commands ensure that systems accept and execute commands in the order intended, execute only authorized commands, and reject unauthorized commands. Cryptographic mechanisms can be used, for example, to authenticate remote commands.

Wireless Access (AC-18)

Description for Wireless Access (AC-18)
a. Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access; and
b. Authorize each type of wireless access to the system prior to allowing such connections.

Discussion for Wireless Access (AC-18)
Wireless technologies include microwave, packet radio (ultra-high frequency or very high frequency), 802.11x, and Bluetooth. Wireless networks use authentication protocols that provide authenticator protection and mutual authentication.

Wireless Access | Authentication and Encryption (AC-18(1))

Description for Wireless Access | Authentication and Encryption (AC-18(1))
Protect wireless access to the system using authentication of [Selection (one or more): users; devices] and encryption.

Discussion for Wireless Access | Authentication and Encryption (AC-18(1))
Wireless networking capabilities represent a significant potential vulnerability that can be exploited by adversaries. To protect systems with wireless access points, strong authentication of users and devices along with strong encryption can reduce susceptibility to threats by adversaries involving wireless technologies.

Access Enforcement | Protection of User and System Information (AC-3(6))

Description for Access Enforcement | Protection of User and System Information (AC-3(6))
[Withdrawn: Incorporated into MP-4 and SC-28.]

Discussion for Access Enforcement | Protection of User and System Information (AC-3(6))

Wireless Access | Disable Wireless Networking (AC-18(3))

Description for Wireless Access | Disable Wireless Networking (AC-18(3))
Disable, when not intended for use, wireless networking capabilities embedded within system components prior to issuance and deployment.

Discussion for Wireless Access | Disable Wireless Networking (AC-18(3))
Wireless networking capabilities that are embedded within system components represent a significant potential vulnerability that can be exploited by adversaries. Disabling wireless capabilities when not needed for essential organizational missions or functions can reduce susceptibility to threats by adversaries involving wireless technologies.

Wireless Access | Restrict Configurations by Users (AC-18(4))

Description for Wireless Access | Restrict Configurations by Users (AC-18(4))
Identify and explicitly authorize users allowed to independently configure wireless networking capabilities.

Discussion for Wireless Access | Restrict Configurations by Users (AC-18(4))
Organizational authorizations to allow selected users to configure wireless networking capabilities are enforced, in part, by the access enforcement mechanisms employed within organizational systems.

Wireless Access | Antennas and Transmission Power Levels (AC-18(5))

Description for Wireless Access | Antennas and Transmission Power Levels (AC-18(5))
Select radio antennas and calibrate transmission power levels to reduce the probability that signals from wireless access points can be received outside of organization-controlled boundaries.

Discussion for Wireless Access | Antennas and Transmission Power Levels (AC-18(5))
Actions that may be taken to limit unauthorized use of wireless communications outside of organization-controlled boundaries include reducing the power of wireless transmissions so that the transmissions are less likely to emit a signal that can be captured outside of the physical perimeters of the organization, employing measures such as emissions security to control wireless emanations, and using directional or beamforming antennas that reduce the likelihood that unintended receivers will be able to intercept signals. Prior to taking such mitigating actions, organizations can conduct periodic wireless surveys to understand the radio frequency profile of organizational systems as well as other systems that may be operating in the area.

Access Control for Mobile Devices (AC-19)

Description for Access Control for Mobile Devices (AC-19)
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.

Discussion for Access Control for Mobile Devices (AC-19)
A mobile device is a computing device that has a small form factor such that it can easily be carried by a single individual; is designed to operate without a physical connection; possesses local, non-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 merely a subset of notebook/desktop systems, depending on 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 and control such devices when outside of controlled areas. Controlled areas are spaces for which organizations provide physical or procedural controls to meet the requirements established for protecting information and systems.
Due to the large variety of mobile devices with different characteristics and capabilities, organizational restrictions may vary for the different classes or types of such devices. Usage restrictions and specific implementation guidance for mobile devices include configuration management, device identification and authentication, implementation of mandatory protective software, scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware. Usage restrictions and authorization to connect may vary among organizational systems. For example, the organization may authorize the connection of mobile devices to its network and impose a set of usage restrictions, while a system owner may withhold authorization for mobile device connection to specific applications or impose additional usage restrictions before allowing mobile device connections to a system. Adequate security for mobile devices goes beyond the requirements specified in AC-19. Many safeguards for mobile devices are reflected in other controls. AC-20 addresses mobile devices that are not organization-controlled.

Information Flow Enforcement | Information Transfers on Interconnected Systems (AC-4(16))

Description for Information Flow Enforcement | Information Transfers on Interconnected Systems (AC-4(16))
[Withdrawn: Incorporated into AC-4.]

Discussion for Information Flow Enforcement | Information Transfers on Interconnected Systems (AC-4(16))

Information Flow Enforcement | Security Attribute Binding (AC-4(18))

Description for Information Flow Enforcement | Security Attribute Binding (AC-4(18))
[Withdrawn: Incorporated into AC-16.]

Discussion for Information Flow Enforcement | Security Attribute Binding (AC-4(18))

Unsuccessful Logon Attempts | Automatic Account Lock (AC-7(1))

Description for Unsuccessful Logon Attempts | Automatic Account Lock (AC-7(1))
[Withdrawn: Incorporated into AC-7.]

Discussion for Unsuccessful Logon Attempts | Automatic Account Lock (AC-7(1))

Access Control for Mobile Devices | Restrictions for Classified Information (AC-19(4))

Description for Access Control for Mobile Devices | Restrictions for Classified Information (AC-19(4))
(a) Prohibit the use of unclassified mobile devices in facilities containing systems processing, storing, or transmitting classified information unless specifically permitted by the authorizing official; and
(b) Enforce the following restrictions on individuals permitted by the authorizing official to use unclassified mobile devices in facilities containing systems processing, storing, or transmitting classified information:
(1) Connection of unclassified mobile devices to classified systems is prohibited;
(2) Connection of unclassified mobile devices to unclassified systems requires approval from the authorizing official;
(3) Use of internal or external modems or wireless interfaces within the unclassified mobile devices is prohibited; and
(4) Unclassified mobile devices and the information stored on those devices are subject to random reviews and inspections by [Assignment: organization-defined security officials], and if classified information is found, the incident handling policy is followed.
(c) Restrict the connection of classified mobile devices to classified systems in accordance with [Assignment: organization-defined security policies].

Discussion for Access Control for Mobile Devices | Restrictions for Classified Information (AC-19(4))
None.

Access Control for Mobile Devices | Full Device or Container-based Encryption (AC-19(5))

Description for Access Control for Mobile Devices | Full Device or Container-based Encryption (AC-19(5))
Employ [Selection: full-device encryption; container-based encryption] to protect the confidentiality and integrity of information on [Assignment: organization-defined mobile devices].

Discussion for Access Control for Mobile Devices | Full Device or Container-based Encryption (AC-19(5))
Container-based encryption provides a more fine-grained approach to data and information encryption on mobile devices, including encrypting selected data structures such as files, records, or fields.

Use of External Systems (AC-20)

Description for Use of External Systems (AC-20)
a. [Selection (one or more): Establish [Assignment: organization-defined terms and conditions]; Identify [Assignment: organization-defined controls asserted to be implemented on external systems]], consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to:
1. Access the system from external systems; and
2. Process, store, or transmit organization-controlled information using external systems; or
b. Prohibit the use of [Assignment: organizationally-defined types of external systems].

Discussion for Use of External Systems (AC-20)
External systems are systems that are used by but not part of organizational systems, and for which the organization has no direct control over the implementation of required controls or the assessment of control effectiveness. External systems include personally owned systems, components, or devices; privately owned computing and communications devices in commercial or public facilities; systems owned or controlled by nonfederal organizations; systems managed by contractors; and federal information systems that are not owned by, operated by, or under the direct supervision or authority of the organization. External systems also include systems owned or operated by other components within the same organization and systems within the organization with different authorization boundaries. Organizations have the option to prohibit the use of any type of external system or prohibit the use of specified types of external systems, (e.g., prohibit the use of any external system that is not organizationally owned or prohibit the use of personally-owned systems).
For some external systems (i.e., systems operated by other organizations), the

trust relationships that have been established between those organizations and the originating organization may be such that no explicit terms and conditions are required. Systems within these organizations may not be considered external. These situations occur when, for example, there are pre-existing information exchange agreements (either implicit or explicit) established between organizations or components or when such agreements are specified by applicable laws, executive orders, directives, regulations, policies, or standards. Authorized individuals include organizational personnel, contractors, or other individuals with authorized access to organizational systems and over which organizations have the authority to impose specific rules of behavior regarding system access. Restrictions that organizations impose on authorized individuals need not be uniform, as the restrictions may vary depending on trust relationships between organizations. Therefore, organizations may choose to impose different security restrictions on contractors than on state, local, or tribal governments.

External systems used to access public interfaces to organizational systems are outside the scope of AC-20. Organizations establish specific terms and conditions for the use of external systems in accordance with organizational security policies and procedures. At a minimum, terms and conditions address the specific types of applications that can be accessed on organizational systems from external systems and the highest security category of information that can be processed, stored, or transmitted on external systems. If the terms and conditions with the owners of the external systems cannot be established, organizations may impose restrictions on organizational personnel using those external systems.

Use of External Systems | Limits on Authorized Use (AC-20(1))

Description for Use of External Systems | Limits on Authorized Use (AC-20(1))
Permit authorized individuals to use an external system to access the system or to process, store, or transmit organization-controlled information only after:
(a) Verification of the implementation of controls on the external system as specified in the organization's security and privacy policies and security and privacy plans; or
(b) Retention of approved system connection or processing agreements with the organizational entity hosting the external system.

Discussion for Use of External Systems | Limits on Authorized Use (AC-20(1))
Limiting authorized use recognizes circumstances where individuals using external systems may need to access organizational systems. Organizations need assurance that the external systems contain the necessary controls so as not to compromise, damage, or otherwise harm organizational systems. Verification that the required controls have been implemented can be achieved by external, independent assessments, attestations, or other means, depending on the confidence level required by organizations.

Use of External Systems | Portable Storage Devices — Restricted Use (AC-20(2))

Description for Use of External Systems | Portable Storage Devices — Restricted Use (AC-20(2))
Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems using [Assignment: organization-defined restrictions].

Discussion for Use of External Systems | Portable Storage Devices — Restricted Use (AC-20(2))
Limits on the use of organization-controlled portable storage devices in external systems include restrictions on how the devices may be used and under what conditions the devices may be used.

Use of External Systems | Non-organizationally Owned Systems — Restricted Use (AC-20(3))

Description for Use of External Systems | Non-organizationally Owned Systems — Restricted Use (AC-20(3))
Restrict the use of non-organizationally owned systems or system components to process, store, or transmit organizational information using [Assignment: organization-defined restrictions].

Discussion for Use of External Systems | Non-organizationally Owned Systems — Restricted Use (AC-20(3))
Non-organizationally owned systems or system components include systems or system components owned by other organizations as well as personally owned devices. There are potential risks to using non-organizationally owned systems or components. In some cases, the risk is sufficiently high as to prohibit such use (see AC-20 b.). 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 approved controls prior to authorizing the connection of non-organizationally owned systems and components; limiting access to types of information, services, or applications; using virtualization techniques to limit processing and storage activities to servers or system components provisioned by the organization; and agreeing to the terms and conditions for usage. Organizations consult with the Office of the General Counsel regarding legal issues

associated with using personally owned devices, including requirements for conducting forensic analyses during investigations after an incident.

Use of External Systems | Network Accessible Storage Devices — Prohibited Use (AC-20(4))

Description for Use of External Systems | Network Accessible Storage Devices — Prohibited Use (AC-20(4))
Prohibit the use of [Assignment: organization-defined network accessible storage devices] in external systems.

Discussion for Use of External Systems | Network Accessible Storage Devices — Prohibited Use (AC-20(4))
Network-accessible storage devices in external systems include online storage devices in public, hybrid, or community cloud-based systems.

Use of External Systems | Portable Storage Devices — Prohibited Use (AC-20(5))

Description for Use of External Systems | Portable Storage Devices — Prohibited Use (AC-20(5))
Prohibit the use of organization-controlled portable storage devices by authorized individuals on external systems.

Discussion for Use of External Systems | Portable Storage Devices — Prohibited Use (AC-20(5))
Limits on the use of organization-controlled portable storage devices in external systems include a complete prohibition of the use of such devices. Prohibiting such use is enforced using technical methods and/or nontechnical (i.e., process-based) methods.

Information Sharing (AC-21)

Description for Information Sharing (AC-21)
a. Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions for [Assignment: organization-defined information sharing circumstances where user discretion is required]; and
b. Employ [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing and collaboration decisions.

Discussion for Information Sharing (AC-21)
Information sharing applies to information that may be restricted in some manner based on some formal or administrative determination. Examples of such information include, contract-sensitive information, classified information related to special access programs or compartments, privileged 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 partners may be defined at the individual, group, or organizational level. Information may be defined by content, type, security category, or special access program or compartment. Access restrictions may include non-disclosure agreements (NDA). Information flow techniques and security attributes may be used to provide automated assistance to users making sharing and collaboration decisions.

Information Sharing | Automated Decision Support (AC-21(1))

Description for Information Sharing | Automated Decision Support (AC-21(1))
Employ [Assignment: organization-defined automated mechanisms] to enforce information-sharing decisions by authorized users based on access authorizations of sharing partners and access restrictions on information to be shared.

Discussion for Information Sharing | Automated Decision Support (AC-21(1))
Automated mechanisms are used to enforce information sharing decisions.

Information Sharing | Information Search and Retrieval (AC-21(2))

Description for Information Sharing | Information Search and Retrieval (AC-21(2))
Implement information search and retrieval services that enforce [Assignment: organization-defined information sharing restrictions].

Discussion for Information Sharing | Information Search and Retrieval (AC-21(2))
Information search and retrieval services identify information system resources relevant to an information need.

Publicly Accessible Content (AC-22)

Description for Publicly Accessible Content (AC-22)
a. Designate individuals authorized to make information publicly accessible;
b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information;
c. Review the proposed content of information prior to posting onto the publicly accessible system to ensure that nonpublic information is not included; and
d. Review the content on the publicly accessible system for nonpublic information [Assignment: organization-defined frequency] and remove such information, if discovered.

Discussion for Publicly Accessible Content (AC-22)
In accordance with applicable laws, executive orders, directives, policies, regulations, standards, and guidelines, the public is not authorized to have access to nonpublic information, including information protected under the PRIVACT and proprietary information. Publicly accessible content addresses systems that are controlled by the organization and accessible to the public, typically without identification or authentication. Posting information on non-organizational systems (e.g., non-organizational 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, publicly accessible content addresses the management of the individuals who make such information publicly accessible.

Data Mining Protection (AC-23)

Description for Data Mining Protection (AC-23)
Employ [Assignment: organization-defined data mining prevention and detection techniques] for [Assignment: organization-defined data storage objects] to detect and protect against unauthorized data mining.

Discussion for Data Mining Protection (AC-23)
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 unanticipated 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 frequency of database queries to increase the work factor needed to determine the contents of databases, limiting types of responses provided to database queries, applying differential privacy techniques or homomorphic encryption, and notifying personnel when atypical 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, AU-13 focuses on monitoring for organizational information that may have been mined or otherwise obtained from data stores and is available as open-source information residing on external sites, such as social networking or social media websites.
EO 13587 requires the establishment of an insider threat program for deterring, detecting, and mitigating insider threats, including the safeguarding of sensitive information from exploitation, compromise, or other unauthorized disclosure.
Data mining protection requires organizations to identify appropriate techniques to prevent and detect unnecessary or unauthorized data mining. Data mining can be used by an insider to collect organizational information for the purpose of exfiltration.

Access Control Decisions (AC-24)

Description for Access Control Decisions (AC-24)
[Selection: Establish procedures; Implement mechanisms] to ensure [Assignment: organization-defined access control decisions] are applied to each access request prior to access enforcement.

Discussion for Access Control Decisions (AC-24)
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 common to have access control decisions and access enforcement implemented by the same entity, it is not required, and it is not always an optimal implementation choice. For some architectures and distributed systems, different entities may make access control decisions and enforce access.

Access Control Decisions | Transmit Access Authorization Information (AC-24(1))

Description for Access Control Decisions | Transmit Access Authorization Information (AC-24(1))
Transmit [Assignment: organization-defined access authorization information] using [Assignment: organization-defined controls] to [Assignment: organization-defined systems] that enforce access control decisions.

Discussion for Access Control Decisions | Transmit Access Authorization Information (AC-24(1))
Authorization processes and access control decisions may occur in separate parts of systems or in separate systems. In such instances, authorization information is transmitted securely (e.g., using cryptographic mechanisms) so that timely access control decisions can be enforced at the appropriate locations. To support the access control decisions, it may be necessary to transmit as part of the access authorization information supporting security and privacy attributes. This is because in distributed systems, there are various access control decisions that need to be made, and different entities make these decisions in a serial fashion, each requiring those attributes to make the decisions. Protecting access authorization information ensures that such information cannot be altered, spoofed, or compromised during transmission.

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

Description for Access Control Decisions | No User or Process Identity (AC-24(2))
Enforce access control decisions based on [Assignment: organization-defined security or privacy attributes] that do not include the identity of the user or process acting on behalf of the user.

Discussion for Access Control Decisions | No User or Process Identity (AC-24(2))
In certain situations, it is important that access control decisions can be made without information regarding the identity of the users issuing the requests. These 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, transmitting such information with the needed degree of assurance may be very expensive or difficult to accomplish. MAC, RBAC, ABAC, and label-based control policies, for example, might not include user identity as an attribute.

Reference Monitor (AC-25)

Description for Reference Monitor (AC-25)
Implement a reference monitor for [Assignment: organization-defined access control policies] that is tamperproof, always invoked, and small enough to be subject to analysis and testing, the completeness of which can be assured.

Discussion for Reference Monitor (AC-25)
A reference monitor is a set of design requirements on a reference validation mechanism that, as a key component of an operating system, enforces an access control policy over all subjects and objects. A reference validation mechanism is always invoked, tamper-proof, and small enough to be subject to analysis and tests, the completeness of which can be assured (i.e., verifiable). Information is represented internally within systems using abstractions known as data structures. Internal data structures can represent different types of entities, both active and passive. Active entities, also known as subjects, are associated with individuals, devices, or processes acting on behalf of individuals. Passive entities, also known as objects, are associated with data structures, such as records, buffers, communications ports, tables, files, and inter-process pipes. Reference monitors enforce access control policies that restrict access to objects based on the identity of subjects or groups to which the subjects belong. The system enforces the access control policy based on the rule set established by the policy. The tamper-proof property of the reference monitor prevents determined adversaries from compromising the functioning of the reference validation mechanism. The always invoked property prevents adversaries from bypassing the mechanism and violating the security policy. The smallness property helps to ensure completeness in the analysis and testing of the mechanism to detect any weaknesses or deficiencies (i.e., latent flaws) that would prevent the enforcement of the security policy.

Policy and Procedures (AT-1)

Description for Policy and Procedures (AT-1)
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] awareness and training policy that:
(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the awareness and training policy and the associated awareness and training controls;
b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the awareness and training policy and procedures; and
c. Review and update the current awareness and training:
1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

Discussion for Policy and Procedures (AT-1)
Awareness and training policy and procedures address the controls in the AT family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of awareness and training policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, 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. Events that may precipitate an update to awareness and training policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Literacy Training and Awareness (AT-2)

Description for Literacy Training and Awareness (AT-2)
a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors):
1. As part of initial training for new users and [Assignment: organization-defined frequency] thereafter; and
2. When required by system changes or following [Assignment: organization-defined events];
b. Employ the following techniques to increase the security and privacy awareness of system users [Assignment: organization-defined awareness techniques];
c. Update literacy training and awareness content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
d. Incorporate lessons learned from internal or external security incidents or breaches into literacy training and awareness techniques.

Discussion for Literacy Training and Awareness (AT-2)
Organizations provide basic and advanced levels of literacy training to system users, including measures to test the knowledge level of users. Organizations determine the content of literacy training and awareness based on specific organizational requirements, the systems to which personnel have authorized access, and work environments (e.g., telework). The content includes an understanding of the need for security and privacy as well as actions by users to maintain security and personal privacy and to respond to suspected incidents. The content addresses the need for operations security and the handling of personally identifiable information.
Awareness techniques include displaying posters, offering supplies inscribed with security and privacy reminders, displaying logon screen messages, generating email advisories or notices from organizational officials, and conducting awareness events. Literacy training after the initial training described in AT-2a.1 is conducted at a minimum frequency consistent with applicable laws, directives, regulations, and policies. Subsequent literacy training may be satisfied by one or more short ad hoc sessions and include topical information on recent attack schemes, changes to organizational security and privacy policies, revised security and privacy expectations, or a subset of topics from the initial training. Updating literacy training and awareness content on a regular basis helps to ensure that the content remains relevant. Events that may precipitate an update to literacy training and awareness content include, but are not limited to, assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Literacy Training and Awareness | Practical Exercises (AT-2(1))

Description for Literacy Training and Awareness | Practical Exercises (AT-2(1))
Provide practical exercises in literacy training that simulate events and incidents.

Discussion for Literacy Training and Awareness | Practical Exercises (AT-2(1))
Practical exercises include no-notice 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.

Literacy Training and Awareness | Insider Threat (AT-2(2))

Description for Literacy Training and Awareness | Insider Threat (AT-2(2))
Provide literacy training on recognizing and reporting potential indicators of insider threat.

Discussion for Literacy Training and Awareness | Insider Threat (AT-2(2))
Potential indicators and possible precursors of insider threat can include behaviors such as inordinate, long-term job dissatisfaction; attempts to gain access to information not required for job performance; unexplained access to financial resources; bullying or harassment of fellow employees; workplace violence; and other serious violations of policies, procedures, directives, regulations, rules, or practices. Literacy training includes how to communicate the concerns of employees and management regarding potential indicators of insider threat through channels established by the organization and in accordance with established policies and procedures. Organizations may consider tailoring 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.

Literacy Training and Awareness | Social Engineering and Mining (AT-2(3))

Description for Literacy Training and Awareness | Social Engineering and Mining (AT-2(3))
Provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining.

Discussion for Literacy Training and Awareness | Social Engineering and Mining (AT-2(3))
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, quid pro quo, thread-jacking, social media exploitation, and tailgating. Social mining is an attempt to gather information about the organization that may be used to support future attacks. Literacy training includes information on how to communicate the concerns of employees and management regarding potential and actual instances of social engineering and data mining through organizational channels based on established policies and procedures.

Literacy Training and Awareness | Suspicious Communications and Anomalous System Behavior (AT-2(4))

Description for Literacy Training and Awareness | Suspicious Communications and Anomalous System Behavior (AT-2(4))
Provide literacy training on recognizing suspicious communications and anomalous behavior in organizational systems using [Assignment: organization-defined indicators of malicious code].

Discussion for Literacy Training and Awareness | Suspicious Communications and Anomalous System Behavior (AT-2(4))
A well-trained workforce provides another organizational control that can be employed as part of a defense-in-depth strategy to protect against malicious code coming into organizations via email or the web applications. Personnel are trained to look for indications of potentially suspicious email (e.g., receiving an unexpected email, receiving an email containing strange or poor grammar, or receiving an email from an unfamiliar sender that appears to be from a known sponsor or contractor). Personnel are also trained on how to respond to suspicious email or web communications. For this process to work effectively, personnel are trained and made aware of what constitutes suspicious communications. Training personnel on how to recognize anomalous behaviors in systems can provide organizations with early warning for the presence of malicious code. Recognition of anomalous behavior by organizational personnel can supplement malicious code detection and protection tools and systems employed by organizations.

Literacy Training and Awareness | Advanced Persistent Threat (AT-2(5))

Description for Literacy Training and Awareness | Advanced Persistent Threat (AT-2(5))
Provide literacy training on the advanced persistent threat.

Discussion for Literacy Training and Awareness | Advanced Persistent Threat (AT-2(5))
An effective way to detect advanced persistent threats (APT) and to preclude successful attacks is to provide specific literacy training for individuals. Threat literacy training includes educating individuals on the various ways that APTs can infiltrate 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.

Literacy Training and Awareness | Cyber Threat Environment (AT-2(6))

Description for Literacy Training and Awareness | Cyber Threat Environment (AT-2(6))
(a) Provide literacy training on the cyber threat environment; and
(b) Reflect current cyber threat information in system operations.

Discussion for Literacy Training and Awareness | Cyber Threat Environment (AT-2(6))
Since threats continue to change over time, threat literacy training by the organization is dynamic. Moreover, threat literacy training is not performed in isolation from the system operations that support organizational mission and business functions.

Role-based Training (AT-3)

Description for Role-based Training (AT-3)
a. 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 changes;
b. Update role-based training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
c. Incorporate lessons learned from internal or external security incidents or breaches into role-based training.

Discussion for Role-based Training (AT-3)
Organizations determine the content of training based on the assigned roles and responsibilities of individuals as well as the security and privacy requirements of organizations and the systems to which personnel have authorized access, including technical training specifically tailored for assigned duties. Roles that may require role-based training include senior leaders or management officials (e.g., head of agency/chief executive officer, chief information officer, senior accountable official for risk management, senior agency information security officer, senior agency official for privacy), system owners; authorizing officials; system security officers; privacy officers; acquisition and procurement officials; enterprise architects; systems engineers; software developers; systems security engineers; privacy engineers; system, network, and database administrators; auditors; personnel conducting configuration management activities; personnel performing verification and validation activities; personnel with access to system-level software; control assessors; personnel with contingency planning and incident response duties; personnel with privacy management responsibilities; and personnel with access to personally identifiable information.
Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical controls. Role-based training also includes policies, procedures, tools, methods, and artifacts for the security and privacy roles defined. Organizations provide the training necessary for individuals to fulfill their responsibilities related to operations and supply chain risk management within the context of organizational security and privacy programs. Role-based training also applies to contractors who provide services to federal agencies. Types of training include web-based and computer-based training, classroom-style training, and hands-on training (including micro-training). Updating role-based training on a regular basis helps to ensure that the content remains relevant and effective. Events that may precipitate an update to role-based training content include, but are not limited to, assessment or audit findings, security incidents or breaches, or changes in

applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Role-based Training | Environmental Controls (AT-3(1))

Description for Role-based Training | Environmental Controls (AT-3(1))
Provide [Assignment: organization-defined personnel or roles] with initial and [Assignment: organization-defined frequency] training in the employment and operation of environmental controls.

Discussion for Role-based Training | Environmental Controls (AT-3(1))
Environmental controls include fire suppression and detection devices or systems, sprinkler systems, handheld fire extinguishers, fixed fire hoses, smoke detectors, temperature or humidity, heating, ventilation, air conditioning, and power within the facility.

Role-based Training | Physical Security Controls (AT-3(2))

Description for Role-based Training | Physical Security Controls (AT-3(2))
Provide [Assignment: organization-defined personnel or roles] with initial and [Assignment: organization-defined frequency] training in the employment and operation of physical security controls.

Discussion for Role-based Training | Physical Security Controls (AT-3(2))
Physical security controls include physical access control devices, physical intrusion and detection alarms, operating procedures for facility security guards, and monitoring or surveillance equipment.

Role-based Training | Practical Exercises (AT-3(3))

Description for Role-based Training | Practical Exercises (AT-3(3))
Provide practical exercises in security and privacy training that reinforce training objectives.

Discussion for Role-based Training | Practical Exercises (AT-3(3))
Practical exercises for security include training for software developers that addresses simulated attacks that exploit common software vulnerabilities or spear or whale phishing attacks targeted at senior leaders or executives. Practical exercises for privacy include modules with quizzes on identifying and processing personally identifiable information in various scenarios or scenarios on conducting privacy impact assessments.

Role-based Training | Suspicious Communications and Anomalous System Behavior (AT-3(4))

Description for Role-based Training | Suspicious Communications and Anomalous System Behavior (AT-3(4))
[Withdrawn: Moved to AT-2(4)].

Discussion for Role-based Training | Suspicious Communications and Anomalous System Behavior (AT-3(4))

Role-based Training | Processing Personally Identifiable Information (AT-3(5))

Description for Role-based Training | Processing Personally Identifiable Information (AT-3(5))
Provide [Assignment: organization-defined personnel or roles] with initial and [Assignment: organization-defined frequency] training in the employment and operation of personally identifiable information processing and transparency controls.

Discussion for Role-based Training | Processing Personally Identifiable Information (AT-3(5))
Personally identifiable information processing and transparency controls include the organization's authority to process personally identifiable information and personally identifiable information processing purposes. Role-based training for federal agencies addresses the types of information that may constitute personally

identifiable information and the risks, considerations, and obligations associated with its processing. Such training also considers the authority to process personally identifiable information documented in privacy policies and notices, system of records notices, computer matching agreements and notices, privacy impact assessments, PRIVACT statements, contracts, information sharing agreements, memoranda of understanding, and/or other documentation.

Training Records (AT-4)

Description for Training Records (AT-4)
a. Document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training; and
b. Retain individual training records for [Assignment: organization-defined time period].

Discussion for Training Records (AT-4)
Documentation for specialized training may be maintained by individual supervisors at the discretion of the organization. The National Archives and Records Administration provides guidance on records retention for federal agencies.

Contacts with Security Groups and Associations (AT-5)

Description for Contacts with Security Groups and Associations (AT-5)
[Withdrawn: Incorporated into PM-15.]

Discussion for Contacts with Security Groups and Associations (AT-5)

Training Feedback (AT-6)

Description for Training Feedback (AT-6)
Provide feedback on organizational training results to the following personnel [Assignment: organization-defined frequency]: [Assignment: organization-defined personnel].

Discussion for Training Feedback (AT-6)
Training feedback includes awareness training results and role-based training results. Training results, especially failures of personnel in critical roles, can be indicative 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 evaluation and update of organizational training described in AT-2b and AT-3b.

Policy and Procedures (AU-1)

Description for Policy and Procedures (AU-1)
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] audit and accountability policy that:
(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls;
b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the audit and accountability policy and procedures; and
c. Review and update the current audit and accountability:
1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

Discussion for Policy and Procedures (AU-1)
Audit and accountability policy and procedures address the controls in the AU family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of audit and accountability policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, 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. Events that may precipitate an update to audit and accountability policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Event Logging (AU-2)

Description for Event Logging (AU-2)
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 to guide 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 (subset of the event types defined in AU-2a.) along with the frequency of (or situation 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 after-the-fact investigations of incidents; and
e. Review and update the event types selected for logging [Assignment: organization-defined frequency].

Discussion for Event Logging (AU-2)
An event is an observable occurrence in a system. The types of events that require logging are those events that are significant and relevant to the security of systems and the privacy of individuals. Event logging also supports specific monitoring and auditing needs. Event types include password changes, failed logons or failed accesses related to systems, security or privacy attribute changes, administrative privilege usage, PIV credential usage, data action changes, query parameters, or external credential usage. In determining the set of event types that require logging, organizations consider the monitoring and auditing appropriate for each of the controls to be implemented. For completeness, event logging includes all protocols that are operational and supported by the system.
To balance monitoring and auditing requirements with other system needs, event logging requires identifying the subset of event types that are logged at a given point in time. For example, organizations may determine that systems need the capability to log every file access successful and unsuccessful, but not activate that capability except for specific circumstances due to the potential burden on system performance. The types of events that organizations desire to be logged may change. Reviewing and updating the set of logged events is necessary to help ensure that the events remain relevant and continue to support the needs of the organization. Organizations consider how the types of logging events can reveal information about individuals that may give rise to privacy risk and how best to mitigate such risks. For example, there is the potential to reveal personally identifiable information in the audit trail, especially if the logging event is based on patterns or time of usage.
Event logging requirements, including the need to log specific event types, may be referenced in other controls and control enhancements. These include AC-2(4), AC-

3(10), AC-6(9), AC-17(1), CM-3f, CM-5(1), IA-3(3)(b), MA-4(1), MP-4(2), PE-3, PM-21, PT-7, RA-8, SC-7(9), SC-7(15), SI-3(8), SI-4(22), SI-7(8), and SI-10(1).
Organizations include event types that are required by applicable laws, executive orders, directives, policies, regulations, standards, and guidelines. Audit records can be generated at various levels, including at the packet level as information traverses the network. Selecting the appropriate level of event logging is an important part of a monitoring and auditing capability and can identify the root causes of problems. When defining event types, organizations consider the logging necessary to cover related event types, such as the steps in distributed, transaction-based processes and the actions that occur in service-oriented architectures.

Non-repudiation | Digital Signatures (AU-10(5))

Description for Non-repudiation | Digital Signatures (AU-10(5))
[Withdrawn: Incorporated into SI-7.]

Discussion for Non-repudiation | Digital Signatures (AU-10(5))

Session Audit | Capture and Record Content (AU-14(2))

Description for Session Audit | Capture and Record Content (AU-14(2))
[Withdrawn: Incorporated into AU-14.]

Discussion for Session Audit | Capture and Record Content (AU-14(2))

Alternate Audit Logging Capability (AU-15)

Description for Alternate Audit Logging Capability (AU-15)
[Withdrawn: Moved to AU-5(5).]

Discussion for Alternate Audit Logging Capability (AU-15)

Event Logging | Compilation of Audit Records from Multiple Sources (AU-2(1))

Description for Event Logging | Compilation of Audit Records from Multiple Sources (AU-2(1))
[Withdrawn: Incorporated into AU-12.]

Discussion for Event Logging | Compilation of Audit Records from Multiple Sources (AU-2(1))

Content of Audit Records (AU-3)

Description for Content of Audit Records (AU-3)
Ensure that audit records contain information that establishes the following:
a. What type of event occurred;
b. When the event occurred;
c. Where the event occurred;
d. Source of the event;
e. Outcome of the event; and
f. Identity of any individuals, subjects, or objects/entities associated with the event.

Discussion for Content of Audit Records (AU-3)
Audit record content that may be necessary to support the auditing function includes event descriptions (item a), time stamps (item b), source and destination addresses (item c), user or process identifiers (items d and f), success or fail indications (item e), and filenames involved (items a, c, e, and f) . Event outcomes include indicators of event success or failure and event-specific results, such as the system security and privacy posture after the event occurred. Organizations consider how audit records can reveal information about individuals that may give rise to privacy risks and how best to mitigate such risks. For example, there is the potential to reveal personally identifiable information in the audit trail, especially if the trail records inputs or is based on patterns or time of usage.

Content of Audit Records | Additional Audit Information (AU-3(1))

Description for Content of Audit Records | Additional Audit Information (AU-3(1))
Generate audit records containing the following additional information: [Assignment: organization-defined additional information].

Discussion for Content of Audit Records | Additional Audit Information (AU-3(1))
The ability to add information generated in audit records is dependent on system functionality to configure the audit record content. Organizations may consider additional information in audit records including, but not limited to, access control or flow control rules invoked and individual identities of group account users. Organizations may also consider limiting additional audit record information to only information that is explicitly needed for audit requirements. This facilitates the use of audit trails and audit logs by not including information in audit records that could potentially be misleading, make it more difficult to locate information of interest, or increase the risk to individuals' privacy.

Event Logging | Selection of Audit Events by Component (AU-2(2))

Description for Event Logging | Selection of Audit Events by Component (AU-2(2))
[Withdrawn: Incorporated into AU-12.]

Discussion for Event Logging | Selection of Audit Events by Component (AU-2(2))

Content of Audit Records | Limit Personally Identifiable Information Elements (AU-3(3))

Description for Content of Audit Records | Limit Personally Identifiable Information Elements (AU-3(3))
Limit personally identifiable information contained in audit records to the following elements identified in the privacy risk assessment: [Assignment: organization-defined elements].

Discussion for Content of Audit Records | Limit Personally Identifiable Information Elements (AU-3(3))
Limiting personally identifiable information in audit records when such information is not needed for operational purposes helps reduce the level of privacy risk created by a system.

Audit Log Storage Capacity (AU-4)

Description for Audit Log Storage Capacity (AU-4)
Allocate audit log storage capacity to accommodate [Assignment: organization-defined audit log retention requirements].

Discussion for Audit Log Storage Capacity (AU-4)
Organizations consider the types of audit logging to be performed and the audit log processing requirements when allocating audit log storage capacity. Allocating sufficient audit log storage capacity reduces the likelihood of such capacity being exceeded and resulting in the potential loss or reduction of audit logging capability.

Audit Log Storage Capacity | Transfer to Alternate Storage (AU-4(1))

Description for Audit Log Storage Capacity | Transfer to Alternate Storage (AU-4(1))
Transfer audit logs [Assignment: organization-defined frequency] to a different system, system component, or media other than the system or system component conducting the logging.

Discussion for Audit Log Storage Capacity | Transfer to Alternate Storage (AU-4(1))
Audit log transfer, also known as off-loading, is a common process in systems with limited audit log storage capacity and thus supports availability of the audit logs. The initial audit log storage is only used in a transitory fashion until the system can communicate with the secondary or alternate system allocated to audit log storage, at which point the audit logs are transferred. Transferring audit logs to alternate storage is similar to AU-9(2) in that audit logs are transferred to a different entity. However, the purpose of selecting AU-9(2) is to protect the confidentiality and integrity of audit records. Organizations can select either control enhancement to obtain the benefit of increased audit log storage capacity

and preserving the confidentiality, integrity, and availability of audit records and logs.

Response to Audit Logging Process Failures (AU-5)

Description for Response to Audit Logging Process Failures (AU-5)
a. Alert [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period] in the event of an audit logging process failure; and
b. Take the following additional actions: [Assignment: organization-defined additional actions].

Discussion for Response to Audit Logging Process Failures (AU-5)
Audit logging process failures include software and hardware errors, failures in audit log capturing mechanisms, and reaching or exceeding audit log storage capacity. Organization-defined actions include overwriting oldest audit records, shutting down the system, and stopping the generation of audit records. Organizations may choose to define additional actions for audit logging process failures based on the type of failure, the location of the failure, the severity of the failure, or a combination of such factors. When the audit logging process failure is related to storage, the response is carried out for the audit log storage repository (i.e., the distinct system component where the audit logs are stored), the system on which the audit logs reside, the total audit log storage capacity of the organization (i.e., all audit log storage repositories combined), or all three. Organizations may decide to take no additional actions after alerting designated roles or personnel.

Response to Audit Logging Process Failures | Storage Capacity Warning (AU-5(1))

Description for Response to Audit Logging Process Failures | Storage Capacity Warning (AU-5(1))
Provide a warning to [Assignment: organization-defined personnel, roles, and/or locations] within [Assignment: organization-defined time period] when allocated audit log storage volume reaches [Assignment: organization-defined percentage] of repository maximum audit log storage capacity.

Discussion for Response to Audit Logging Process Failures | Storage Capacity Warning (AU-5(1))
Organizations may have multiple audit log storage repositories distributed across multiple system components with each repository having different storage volume capacities.

Response to Audit Logging Process Failures | Real-time Alerts (AU-5(2))

Description for Response to Audit Logging Process Failures | Real-time Alerts (AU-5(2))
Provide an alert within [Assignment: organization-defined real-time period] to [Assignment: organization-defined personnel, roles, and/or locations] when the following audit failure events occur: [Assignment: organization-defined audit logging failure events requiring real-time alerts].

Discussion for Response to Audit Logging Process Failures | Real-time Alerts (AU-5(2))
Alerts provide organizations with urgent messages. Real-time alerts provide these messages at information technology speed (i.e., the time from event detection to alert occurs in seconds or less).

Response to Audit Logging Process Failures | Configurable Traffic Volume Thresholds (AU-5(3))

Description for Response to Audit Logging Process Failures | Configurable Traffic Volume Thresholds (AU-5(3))
Enforce configurable network communications traffic volume thresholds reflecting limits on audit log storage capacity and [Selection: reject; delay] network traffic above those thresholds.

Discussion for Response to Audit Logging Process Failures | Configurable Traffic Volume Thresholds (AU-5(3))
Organizations have the capability to reject or delay the processing of network communications traffic if audit logging information about such traffic is determined to exceed the storage capacity of the system audit logging function. The rejection or delay response is triggered by the established organizational traffic volume thresholds that can be adjusted based on changes to audit log storage capacity.

Response to Audit Logging Process Failures | Shutdown on Failure (AU-5(4))

Description for Response to Audit Logging Process Failures | Shutdown on Failure (AU-5(4))
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 failures], unless an alternate audit logging capability exists.

Discussion for Response to Audit Logging Process Failures | Shutdown on Failure (AU-5(4))
Organizations determine the types of audit logging failures that can trigger automatic system shutdowns or degraded operations. Because of the importance of ensuring mission and business continuity, organizations may determine that the nature of the audit logging failure is not so severe that it warrants a complete shutdown of the system supporting the core organizational mission and business functions. In those instances, partial system shutdowns or operating in a degraded mode with reduced capability may be viable alternatives.

Response to Audit Logging Process Failures | Alternate Audit Logging Capability (AU-5(5))

Description for Response to Audit Logging Process Failures | Alternate Audit Logging Capability (AU-5(5))
Provide an alternate audit logging capability in the event of a failure in primary audit logging capability that implements [Assignment: organization-defined alternate audit logging functionality].

Discussion for Response to Audit Logging Process Failures | Alternate Audit Logging Capability (AU-5(5))
Since an alternate audit logging capability may be a short-term protection solution employed 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 (AU-6)

Description for Audit Record Review, Analysis, and Reporting (AU-6)
a. Review and analyze system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity] and the potential impact of the inappropriate or unusual activity;
b. Report findings to [Assignment: organization-defined personnel or roles]; and
c. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.

Discussion for Audit Record Review, Analysis, and Reporting (AU-6)
Audit record review, analysis, and reporting covers information security- and privacy-related logging performed by organizations, including logging that results from the monitoring of account usage, remote access, wireless connectivity, mobile device connection, configuration settings, system component inventory, use of maintenance tools and non-local maintenance, physical access, temperature and humidity, equipment delivery and removal, communications at system interfaces, and use of mobile code or Voice over Internet Protocol (VoIP). Findings can be reported to organizational entities that include the incident response team, help desk, and security or privacy offices. If organizations are prohibited from reviewing and analyzing audit records or unable to conduct such activities, the review or analysis may be carried out by other organizations granted such

authority. The frequency, scope, and/or depth of the audit record review, analysis, and reporting may be adjusted to meet organizational needs based on new information received.

Audit Record Review, Analysis, and Reporting | Automated Process Integration (AU-6(1))

Description for Audit Record Review, Analysis, and Reporting | Automated Process Integration (AU-6(1))
Integrate audit record review, analysis, and reporting processes using [Assignment: organization-defined automated mechanisms].

Discussion for Audit Record Review, Analysis, and Reporting | Automated Process Integration (AU-6(1))
Organizational processes that benefit from integrated audit record review, analysis, and reporting include incident response, continuous monitoring, contingency planning, investigation and response to suspicious activities, and Inspector General audits.

Event Logging | Reviews and Updates (AU-2(3))

Description for Event Logging | Reviews and Updates (AU-2(3))
[Withdrawn: Incorporated into AU-2.]

Discussion for Event Logging | Reviews and Updates (AU-2(3))

Audit Record Review, Analysis, and Reporting | Correlate Audit Record Repositories (AU-6(3))

Description for Audit Record Review, Analysis, and Reporting | Correlate Audit Record Repositories (AU-6(3))
Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.

Discussion for Audit Record Review, Analysis, and Reporting | Correlate Audit Record Repositories (AU-6(3))
Organization-wide situational awareness includes awareness across all three levels of risk management (i.e., organizational level, mission/business process level, and information system level) and supports cross-organization awareness.

Audit Record Review, Analysis, and Reporting | Central Review and Analysis (AU-6(4))

Description for Audit Record Review, Analysis, and Reporting | Central Review and Analysis (AU-6(4))
Provide and implement the capability to centrally review and analyze audit records from multiple components within the system.

Discussion for Audit Record Review, Analysis, and Reporting | Central Review and Analysis (AU-6(4))
Automated mechanisms for centralized reviews and analyses include Security Information and Event Management products.

Audit Record Review, Analysis, and Reporting | Integrated Analysis of Audit Records (AU-6(5))

Description for Audit Record Review, Analysis, and Reporting | Integrated Analysis of Audit Records (AU-6(5))
Integrate analysis of audit records with analysis of [Selection (one or more): vulnerability scanning information; performance data; system monitoring information; [Assignment: organization-defined data/information collected from other sources]] to further enhance the ability to identify inappropriate or unusual activity.

Discussion for Audit Record Review, Analysis, and Reporting | Integrated Analysis of Audit Records (AU-6(5))
Integrated analysis of audit records does not require vulnerability scanning, the generation of performance data, or system monitoring. Rather, integrated analysis requires that the analysis of information generated by scanning, monitoring, or other data collection activities is integrated with the analysis of audit record information. Security Information and Event Management tools can facilitate audit record aggregation or consolidation from multiple system components as well as audit record correlation and analysis. The use of standardized audit record analysis scripts developed by organizations (with localized script adjustments, as necessary) provides more cost-effective approaches for analyzing audit record information collected. The correlation of audit record information with vulnerability scanning information is important in determining the veracity of vulnerability scans of the system and in correlating attack detection events with scanning results. Correlation with performance data can uncover denial-of-service attacks or other types of attacks that result in the unauthorized use of resources. Correlation with system monitoring information can assist in uncovering attacks and in better relating audit information to operational situations.

Audit Record Review, Analysis, and Reporting | Correlation with Physical Monitoring (AU-6(6))

Description for Audit Record Review, Analysis, and Reporting | Correlation with Physical Monitoring (AU-6(6))
Correlate information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.

Discussion for Audit Record Review, Analysis, and Reporting | Correlation with Physical Monitoring (AU-6(6))
The correlation of physical audit record information and the audit records from systems may assist organizations in identifying suspicious behavior or supporting evidence of such behavior. For example, the correlation of an individual's identity for logical access to certain systems with the additional physical security information that the individual was present at the facility when the logical access occurred may be useful in investigations.

Audit Record Review, Analysis, and Reporting | Permitted Actions (AU-6(7))

Description for Audit Record Review, Analysis, and Reporting | Permitted Actions (AU-6(7))
Specify the permitted actions for each [Selection (one or more): system process; role; user] associated with the review, analysis, and reporting of audit record information.

Discussion for Audit Record Review, Analysis, and Reporting | Permitted Actions (AU-6(7))
Organizations specify permitted actions for system processes, roles, and users associated with the review, analysis, and reporting of audit records through system account management activities. Specifying permitted actions on audit record information is a way to enforce the principle of least privilege. Permitted actions are enforced by the system and include read, write, execute, append, and delete.

Audit Record Review, Analysis, and Reporting | Full Text Analysis of Privileged Commands (AU-6(8))

Description for Audit Record Review, Analysis, and Reporting | Full Text Analysis of Privileged Commands (AU-6(8))
Perform a full text analysis of logged privileged commands in a physically distinct component or subsystem of the system, or other system that is dedicated to that analysis.

Discussion for Audit Record Review, Analysis, and Reporting | Full Text Analysis of Privileged Commands (AU-6(8))
Full text analysis of privileged commands requires a distinct environment for the analysis of audit record information related to privileged users without compromising such information on the system where the users have elevated privileges, including the capability to execute privileged commands. Full text analysis refers to analysis that considers the full text of privileged commands (i.e., commands and parameters) as opposed to analysis that considers only the name of the command. Full text analysis includes the use of pattern matching and heuristics.

Audit Record Review, Analysis, and Reporting | Correlation with Information from Nontechnical Sources (AU-6(9))

Description for Audit Record Review, Analysis, and Reporting | Correlation with Information from Nontechnical Sources (AU-6(9))
Correlate information from nontechnical sources with audit record information to enhance organization-wide situational awareness.

Discussion for Audit Record Review, Analysis, and Reporting | Correlation with Information from Nontechnical Sources (AU-6(9))
Nontechnical sources include records that document organizational policy violations related to harassment incidents and the improper use of information assets. Such information can lead to a directed analytical effort to detect potential malicious insider activity. Organizations limit access to information that is available from nontechnical sources due to its sensitive nature. Limited access minimizes the potential for inadvertent release of privacy-related information to individuals who do not have a need to know. The correlation of information from nontechnical sources with audit record information generally occurs only when individuals are suspected of being involved in an incident. Organizations obtain legal advice prior to initiating such actions.

Event Logging | Privileged Functions (AU-2(4))

Description for Event Logging | Privileged Functions (AU-2(4))
[Withdrawn: Incorporated into AC-6(9).]

Discussion for Event Logging | Privileged Functions (AU-2(4))

Audit Record Reduction and Report Generation (AU-7)

Description for Audit Record Reduction and Report Generation (AU-7)
Provide and implement an audit record reduction and report generation capability that:
a. Supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of incidents; and
b. Does not alter the original content or time ordering of audit records.

Discussion for Audit Record Reduction and Report Generation (AU-7)
Audit record reduction is a process that manipulates collected audit log information and organizes it into 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 that conduct 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 timestamp in the record is insufficient.

Audit Record Reduction and Report Generation | Automatic Processing (AU-7(1))

Description for Audit Record Reduction and Report Generation | Automatic Processing (AU-7(1))
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].

Discussion for Audit Record Reduction and Report Generation | Automatic Processing (AU-7(1))
Events of interest can be identified by the content of audit records, including system resources involved, information objects accessed, identities of individuals, event types, event locations, event dates and times, Internet Protocol addresses involved, or event success or failure. Organizations may define event criteria to any degree of granularity required, such as locations selectable by a general networking location or by specific system component.

Content of Audit Records | Centralized Management of Planned Audit Record Content (AU-3(2))

Description for Content of Audit Records | Centralized Management of Planned Audit Record Content (AU-3(2))
[Withdrawn: Incorporated into PL-9.]

Discussion for Content of Audit Records | Centralized Management of Planned Audit Record Content (AU-3(2))

Time Stamps (AU-8)

Description for Time Stamps (AU-8)
a. Use internal system clocks to generate time stamps for audit records; and
b. Record time stamps for audit records that meet [Assignment: organization-defined granularity of time measurement] and that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.

Discussion for Time Stamps (AU-8)
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 (e.g., 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 those capabilities.

Audit Record Review, Analysis, and Reporting | Audit Level Adjustment (AU-6(10))

Description for Audit Record Review, Analysis, and Reporting | Audit Level Adjustment (AU-6(10))
[Withdrawn: Incorporated into AU-6.]

Discussion for Audit Record Review, Analysis, and Reporting | Audit Level Adjustment (AU-6(10))

Audit Record Review, Analysis, and Reporting | Automated Security Alerts (AU-6(2))

Description for Audit Record Review, Analysis, and Reporting | Automated Security Alerts (AU-6(2))
[Withdrawn: Incorporated into SI-4.]

Discussion for Audit Record Review, Analysis, and Reporting | Automated Security Alerts (AU-6(2))

Protection of Audit Information (AU-9)

Description for Protection of Audit Information (AU-9)
a. Protect audit information and audit logging tools from unauthorized access, modification, and deletion; and
b. Alert [Assignment: organization-defined personnel or roles] upon detection of unauthorized access, modification, or deletion of audit information.

Discussion for Protection of Audit Information (AU-9)
Audit information includes all information needed to successfully audit system activity, such as audit records, audit log settings, audit reports, and personally identifiable information. Audit logging tools are those programs and devices used to conduct system audit and logging activities. Protection of audit information

focuses on technical protection and limits the ability to access and execute audit logging tools to authorized individuals. Physical protection of audit information is addressed by both media protection controls and physical and environmental protection controls.

Protection of Audit Information | Hardware Write-once Media (AU-9(1))

Description for Protection of Audit Information | Hardware Write-once Media (AU-9(1))
Write audit trails to hardware-enforced, write-once media.

Discussion for Protection of Audit Information | Hardware Write-once Media (AU-9(1))
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 represents 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, read-many (WORM) media includes Compact Disc-Recordable (CD-R), Blu-Ray Disc Recordable (BD-R), and Digital Versatile Disc-Recordable (DVD-R). In contrast, the use of switchable write-protection media, such as tape cartridges, Universal Serial Bus (USB) drives, Compact Disc Re-Writeable (CD-RW), and Digital Versatile Disc-Read Write (DVD-RW) results in write-protected but not write-once media.

Protection of Audit Information | Store on Separate Physical Systems or Components (AU-9(2))

Description for Protection of Audit Information | Store on Separate Physical Systems or Components (AU-9(2))
Store audit records [Assignment: organization-defined frequency] in a repository that is part of a physically different system or system component than the system or component being audited.

Discussion for Protection of Audit Information | Store on Separate Physical Systems or Components (AU-9(2))
Storing audit records in a repository separate from the audited system or system component helps to ensure that a compromise 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 organization-wide activity. Storing audit records on separate systems or components applies to initial generation as well as backup or long-term storage of audit records.

Protection of Audit Information | Cryptographic Protection (AU-9(3))

Description for Protection of Audit Information | Cryptographic Protection (AU-9(3))
Implement cryptographic mechanisms to protect the integrity of audit information and audit tools.

Discussion for Protection of Audit Information | Cryptographic Protection (AU-9(3))
Cryptographic mechanisms used for protecting the integrity of audit information include signed hash functions using asymmetric cryptography. This enables the distribution of the public key to verify the hash information while maintaining the confidentiality of the secret key used to generate the hash.

Protection of Audit Information | Access by Subset of Privileged Users (AU-9(4))

Description for Protection of Audit Information | Access by Subset of Privileged Users (AU-9(4))
Authorize access to management of audit logging functionality to only [Assignment: organization-defined subset of privileged users or roles].

Discussion for Protection of Audit Information | Access by Subset of Privileged Users (AU-9(4))
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. Requiring privileged access to be further defined between audit-related privileges and other privileges limits the number of users or roles with audit-related privileges.

Protection of Audit Information | Dual Authorization (AU-9(5))

Description for Protection of Audit Information | Dual Authorization (AU-9(5))
Enforce dual authorization for [Selection (one or more): movement; deletion] of [Assignment: organization-defined audit information].

Discussion for Protection of Audit Information | Dual Authorization (AU-9(5))
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.

Protection of Audit Information | Read-only Access (AU-9(6))

Description for Protection of Audit Information | Read-only Access (AU-9(6))
Authorize read-only access to audit information to [Assignment: organization-defined subset of privileged users or roles].

Discussion for Protection of Audit Information | Read-only Access (AU-9(6))
Restricting privileged user or role authorizations to read-only helps to limit the potential damage to organizations that could be initiated by such users or roles, such as deleting audit records to cover up malicious activity.

Protection of Audit Information | Store on Component with Different Operating System (AU-9(7))

Description for Protection of Audit Information | Store on Component with Different Operating System (AU-9(7))
Store audit information on a component running a different operating system than the system or component being audited.

Discussion for Protection of Audit Information | Store on Component with Different Operating System (AU-9(7))
Storing auditing 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.

Non-repudiation (AU-10)

Description for Non-repudiation (AU-10)
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].

Discussion for Non-repudiation (AU-10)
Types of individual actions covered by non-repudiation include creating information, sending and receiving messages, and approving information. Non-repudiation protects against claims by authors of not having authored certain documents, senders of not having transmitted 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 if an individual took specific actions (e.g., sending an email, signing a contract, approving a procurement request, or receiving specific information). Organizations obtain non-repudiation services by employing various techniques or mechanisms, including digital signatures and digital message receipts.

Non-repudiation | Association of Identities (AU-10(1))

Description for Non-repudiation | Association of Identities (AU-10(1))
(a) Bind the identity of the information producer with the information to [Assignment: organization-defined strength of binding]; and
(b) Provide the means for authorized individuals to determine the identity of the producer of the information.

Discussion for Non-repudiation | Association of Identities (AU-10(1))
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 attribute binding between the information producer and the information based on the security category of the information and other relevant risk factors.

Non-repudiation | Validate Binding of Information Producer Identity (AU-10(2))

Description for Non-repudiation | Validate Binding of Information Producer Identity (AU-10(2))
(a) Validate the binding of the information producer identity to the information at [Assignment: organization-defined frequency]; and
(b) Perform [Assignment: organization-defined actions] in the event of a validation error.

Discussion for Non-repudiation | Validate Binding of Information Producer Identity (AU-10(2))
Validating the binding of the information producer identity to the information prevents the modification of information between production and review. The validation of bindings can be achieved by, for example, using cryptographic checksums. Organizations determine if validations are in response to user requests or generated automatically.

Non-repudiation | Chain of Custody (AU-10(3))

Description for Non-repudiation | Chain of Custody (AU-10(3))
Maintain reviewer or releaser credentials within the established chain of custody for information reviewed or released.

Discussion for Non-repudiation | Chain of Custody (AU-10(3))
Chain of custody is a process that tracks the movement of evidence through its collection, safeguarding, and analysis life cycle by documenting each individual who handled the evidence, the date and time the evidence was collected or transferred, and the purpose for the transfer. If the reviewer is a human or if the review function is automated but separate from the release or transfer function, the system associates the identity of the reviewer of the information to be released with the information and the information label. In the case of human reviews, maintaining the credentials of reviewers or releasers provides the organization with the means to identify who reviewed and released the information. In the case of automated reviews, it ensures that only approved review functions are used.

Non-repudiation | Validate Binding of Information Reviewer Identity (AU-10(4))

Description for Non-repudiation | Validate Binding of Information Reviewer Identity (AU-10(4))
(a) Validate the binding of the information reviewer identity to the information at the transfer or release points prior to release or transfer between [Assignment: organization-defined security domains]; and
(b) Perform [Assignment: organization-defined actions] in the event of a validation error.

Discussion for Non-repudiation | Validate Binding of Information Reviewer Identity (AU-10(4))
Validating the binding of the information reviewer identity to the information at transfer or release points prevents the unauthorized modification of information between review and the transfer or release. The validation of bindings can be achieved by using cryptographic checksums. Organizations determine if validations are in response to user requests or generated automatically.

Audit Record Reduction and Report Generation | Automatic Sort and Search (AU-7(2))

Description for Audit Record Reduction and Report Generation | Automatic Sort and Search (AU-7(2))
[Withdrawn: Incorporated into AU-7(1).]

Discussion for Audit Record Reduction and Report Generation | Automatic Sort and Search (AU-7(2))

Audit Record Retention (AU-11)

Description for Audit Record Retention (AU-11)
Retain audit records for [Assignment: organization-defined time period consistent with records retention policy] to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements.

Discussion for Audit Record Retention (AU-11)
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 Act (FOIA) requests, subpoenas, and law enforcement actions. Organizations develop standard categories of audit records relative to such types of actions and standard response processes for each type of action. The National Archives and Records Administration (NARA) General Records Schedules provide federal policy on records retention.

Audit Record Retention | Long-term Retrieval Capability (AU-11(1))

Description for Audit Record Retention | Long-term Retrieval Capability (AU-11(1))
Employ [Assignment: organization-defined measures] to ensure that long-term audit records generated by the system can be retrieved.

Discussion for Audit Record Retention | Long-term Retrieval Capability (AU-11(1))
Organizations need to access and read audit records requiring long-term storage (on the order of years). Measures employed to help facilitate the retrieval of audit records include converting records to newer formats, retaining equipment capable of reading the records, and retaining the necessary documentation to help personnel understand how to interpret the records.

Audit Record Generation (AU-12)

Description for Audit Record Generation (AU-12)
a. Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2a on [Assignment: organization-defined system components];
b. Allow [Assignment: organization-defined personnel or roles] to select the event types that are to be logged by specific components of the system; and
c. Generate audit records for the event types defined in AU-2c that include the audit record content defined in AU-3.

Discussion for Audit Record Generation (AU-12)
Audit records can be generated from many different system components. The event types specified in AU-2d are the event types for which audit logs are to be generated and are a subset of all event types for which the system can generate audit records.

Audit Record Generation | System-wide and Time-correlated Audit Trail (AU-12(1))

Description for Audit Record Generation | System-wide and Time-correlated Audit Trail (AU-12(1))
Compile audit records from [Assignment: organization-defined system components] into a system-wide (logical or physical) audit trail that is time-correlated to within [Assignment: organization-defined level of tolerance for the relationship between time stamps of individual records in the audit trail].

Discussion for Audit Record Generation | System-wide and Time-correlated Audit Trail (AU-12(1))
Audit trails are time-correlated if the time stamps in the individual audit records can be reliably related to the time stamps in other audit records to achieve a time ordering of the records within organizational tolerances.

Audit Record Generation | Standardized Formats (AU-12(2))

Description for Audit Record Generation | Standardized Formats (AU-12(2))
Produce a system-wide (logical or physical) audit trail composed of audit records in a standardized format.

Discussion for Audit Record Generation | Standardized Formats (AU-12(2))
Audit records that follow common standards promote interoperability and information exchange between devices and systems. Promoting interoperability and information exchange facilitates the production of event information that can be readily analyzed and correlated. If logging mechanisms do not conform to standardized formats, systems may convert individual audit records into standardized formats when compiling system-wide audit trails.

Audit Record Generation | Changes by Authorized Individuals (AU-12(3))

Description for Audit Record Generation | Changes by Authorized Individuals (AU-12(3))
Provide and implement the capability for [Assignment: organization-defined individuals or roles] to change the logging to be performed on [Assignment: organization-defined system components] based on [Assignment: organization-defined selectable event criteria] within [Assignment: organization-defined time thresholds].

Discussion for Audit Record Generation | Changes by Authorized Individuals (AU-12(3))
Permitting authorized individuals to make changes to system logging enables organizations to extend or limit logging as necessary to meet organizational requirements. Logging that is limited to conserve system resources may be extended (either temporarily or permanently) to address certain threat situations. In addition, logging may be limited to a specific set of event types to facilitate audit reduction, analysis, and reporting. Organizations can establish time thresholds in which logging actions are changed (e.g., near real-time, within minutes, or within hours).

Audit Record Generation | Query Parameter Audits of Personally Identifiable Information (AU-12(4))

Description for Audit Record Generation | Query Parameter Audits of Personally Identifiable Information (AU-12(4))
Provide and implement the capability for auditing the parameters of user query events for data sets containing personally identifiable information.

Discussion for Audit Record Generation | Query Parameter Audits of Personally Identifiable Information (AU-12(4))
Query parameters are explicit criteria that an individual or automated system submits to a system to retrieve data. Auditing of query parameters for datasets that contain personally identifiable information augments the capability of an organization to track and understand the access, usage, or sharing of personally identifiable information by authorized personnel.

Monitoring for Information Disclosure (AU-13)

Description for Monitoring for Information Disclosure (AU-13)
a. Monitor [Assignment: organization-defined open-source information and/or information sites] [Assignment: organization-defined frequency] for evidence of unauthorized disclosure of organizational information; and
b. If an information disclosure is discovered:
1. Notify [Assignment: organization-defined personnel or roles]; and
2. Take the following additional actions: [Assignment: organization-defined additional actions].

Discussion for Monitoring for Information Disclosure (AU-13)
Unauthorized disclosure of information is a form of data leakage. Open-source information includes social networking sites and code-sharing platforms and repositories. Examples of organizational information include personally identifiable information retained by the organization or proprietary information generated by the organization.

Monitoring for Information Disclosure | Use of Automated Tools (AU-13(1))

Description for Monitoring for Information Disclosure | Use of Automated Tools (AU-13(1))
Monitor open-source information and information sites using [Assignment: organization-defined automated mechanisms].

Discussion for Monitoring for Information Disclosure | Use of Automated Tools (AU-13(1))
Automated mechanisms include commercial services that provide notifications and alerts to organizations and automated scripts to monitor new posts on websites.

Monitoring for Information Disclosure | Review of Monitored Sites (AU-13(2))

Description for Monitoring for Information Disclosure | Review of Monitored Sites (AU-13(2))
Review the list of open-source information sites being monitored [Assignment: organization-defined frequency].

Discussion for Monitoring for Information Disclosure | Review of Monitored Sites (AU-13(2))
Reviewing the current list of open-source information sites being monitored on a regular basis helps to ensure that the selected sites remain relevant. The review also provides the opportunity to add new open-source information sites with the potential to provide evidence of unauthorized disclosure of organizational information. The list of sites monitored can be guided and informed by threat intelligence of other credible sources of information.

Monitoring for Information Disclosure | Unauthorized Replication of Information (AU-13(3))

Description for Monitoring for Information Disclosure | Unauthorized Replication of Information (AU-13(3))
Employ discovery techniques, processes, and tools to determine if external entities are replicating organizational information in an unauthorized manner.

Discussion for Monitoring for Information Disclosure | Unauthorized Replication of Information (AU-13(3))
The unauthorized use or replication of organizational information by external entities can cause adverse impacts on organizational operations and assets, including damage to reputation. Such activity can include the replication of an organizational website by an adversary or hostile threat actor who attempts to impersonate the web-hosting organization. Discovery tools, techniques, and processes used to determine if external entities are replicating organizational information in an unauthorized manner include scanning external websites, monitoring social media, and training staff to recognize the unauthorized use of organizational information.

Session Audit (AU-14)

Description for Session Audit (AU-14)
a. Provide and implement the capability for [Assignment: organization-defined users or roles] to [Selection (one or more): record; view; hear; log] the content of a user session under [Assignment: organization-defined circumstances]; and
b. Develop, integrate, and use session auditing activities in consultation with legal counsel and in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Discussion for Session Audit (AU-14)
Session audits can include monitoring keystrokes, tracking websites visited, and recording information and/or file transfers. Session audit capability is implemented in addition to event logging and may involve implementation of specialized session capture technology. Organizations consider how session auditing can reveal information about individuals that may give rise to privacy risk as well as how to mitigate those risks. Because session auditing can impact system and network performance, organizations activate the capability under well-defined situations (e.g., the organization is suspicious of a specific individual). Organizations consult with legal counsel, civil liberties officials, and privacy officials to ensure that any legal, privacy, civil rights, or civil liberties issues, including the use of personally identifiable information, are appropriately addressed.

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

Description for Session Audit | System Start-up (AU-14(1))
Initiate session audits automatically at system start-up.

Discussion for Session Audit | System Start-up (AU-14(1))
The automatic initiation of session audits at startup helps to ensure that the information being captured on selected individuals is complete and not subject to compromise through tampering by malicious threat actors.

Time Stamps | Synchronization with Authoritative Time Source (AU-8(1))

Description for Time Stamps | Synchronization with Authoritative Time Source (AU-8(1))
[Withdrawn: Moved to SC-45(1).]

Discussion for Time Stamps | Synchronization with Authoritative Time Source (AU-8(1))

Session Audit | Remote Viewing and Listening (AU-14(3))

Description for Session Audit | Remote Viewing and Listening (AU-14(3))
Provide and implement the capability for authorized users to remotely view and hear content related to an established user session in real time.

Discussion for Session Audit | Remote Viewing and Listening (AU-14(3))
None.

Time Stamps | Secondary Authoritative Time Source (AU-8(2))

Description for Time Stamps | Secondary Authoritative Time Source (AU-8(2))
[Withdrawn: Moved to SC-45(2).]

Discussion for Time Stamps | Secondary Authoritative Time Source (AU-8(2))

Cross-organizational Audit Logging (AU-16)

Description for Cross-organizational Audit Logging (AU-16)
Employ [Assignment: organization-defined methods] for coordinating [Assignment: organization-defined audit information] among external organizations when audit information is transmitted across organizational boundaries.

Discussion for Cross-organizational Audit Logging (AU-16)
When organizations use systems or services of external organizations, the audit logging capability necessitates a coordinated, cross-organization approach. For example, maintaining the identity of individuals who request specific services across organizational boundaries may often be difficult, and doing so may prove to have significant performance and privacy ramifications. Therefore, it is often the case that cross-organizational audit logging simply captures the identity of individuals who issue requests at the initial system, and subsequent systems record that the requests originated from authorized individuals. Organizations consider including processes for coordinating audit information requirements and protection of audit information in information exchange agreements.

Cross-organizational Audit Logging | Identity Preservation (AU-16(1))

Description for Cross-organizational Audit Logging | Identity Preservation (AU-16(1))
Preserve the identity of individuals in cross-organizational audit trails.

Discussion for Cross-organizational Audit Logging | Identity Preservation (AU-16(1))
Identity preservation is applied when there is a need to be able to trace actions that are performed across organizational boundaries to a specific individual.

Cross-organizational Audit Logging | Sharing of Audit Information (AU-16(2))

Description for Cross-organizational Audit Logging | Sharing of Audit Information (AU-16(2))
Provide cross-organizational audit information to [Assignment: organization-defined organizations] based on [Assignment: organization-defined cross-organizational sharing agreements].

Discussion for Cross-organizational Audit Logging | Sharing of Audit Information (AU-16(2))
Due to the distributed nature of the audit information, cross-organization sharing of audit information may be essential for effective analysis of the auditing being performed. For example, the audit records of one organization may not provide sufficient information to determine the appropriate or inappropriate use of organizational information resources by individuals in other organizations. In some instances, only individuals' home organizations have the appropriate knowledge to make such determinations, thus requiring the sharing of audit information among organizations.

Cross-organizational Audit Logging | Disassociability (AU-16(3))

Description for Cross-organizational Audit Logging | Disassociability (AU-16(3))
Implement [Assignment: organization-defined measures] to disassociate individuals from audit information transmitted across organizational boundaries.

Discussion for Cross-organizational Audit Logging | Disassociability (AU-16(3))
Preserving identities in audit trails could have privacy ramifications, such as enabling the tracking and profiling of individuals, but may not be operationally necessary. These risks could be further amplified when transmitting information across organizational boundaries. Implementing privacy-enhancing cryptographic techniques can disassociate individuals from audit information and reduce privacy risk while maintaining accountability.

Policy and Procedures (CA-1)

Description for Policy and Procedures (CA-1)
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] assessment, authorization, and monitoring policy that:
(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the assessment, authorization, and monitoring policy and the associated assessment, authorization, and monitoring controls;
b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the assessment, authorization, and monitoring policy and procedures; and
c. Review and update the current assessment, authorization, and monitoring:
1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

Discussion for Policy and Procedures (CA-1)
Assessment, authorization, and monitoring policy and procedures address the controls in the CA family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of assessment, authorization, and monitoring policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, 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. Events that may precipitate an update to assessment, authorization, and monitoring policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and

guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Control Assessments (CA-2)

Description for Control Assessments (CA-2)
a. Select the appropriate assessor or assessment team for the type of assessment to be conducted;
b. Develop a control assessment plan that describes the scope of the assessment including:
1. Controls and control enhancements under assessment;
2. Assessment procedures to be used to determine control effectiveness; and
3. Assessment environment, assessment team, and assessment roles and responsibilities;
c. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment;
d. 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;
e. Produce a control assessment report that document the results of the assessment; and
f. Provide the results of the control assessment to [Assignment: organization-defined individuals or roles].

Discussion for Control Assessments (CA-2)
Organizations ensure that control assessors possess the required skills and technical expertise to develop effective assessment plans and to conduct assessments of system-specific, hybrid, common, and program management controls, as appropriate. The required skills include general knowledge of risk management concepts and approaches as well as comprehensive knowledge of and experience with the hardware, software, and firmware system components implemented.
Organizations assess controls in systems and the environments in which those systems operate as part of initial and ongoing authorizations, continuous monitoring, FISMA annual assessments, system design and development, systems security engineering, privacy engineering, and the system development life cycle. Assessments help to ensure that organizations meet information security and privacy requirements, identify weaknesses and deficiencies in the system design and development process, provide essential information needed to make risk-based decisions as part of authorization processes, and comply with vulnerability mitigation procedures. Organizations conduct assessments on the implemented controls as documented in security and privacy plans. Assessments can also be conducted throughout the system development life cycle as part of systems engineering and systems security engineering processes. The design for controls can be assessed as RFPs are developed, responses assessed, and design reviews conducted. If a design to implement controls and subsequent implementation in

accordance with the design are assessed during development, the final control testing can be a simple confirmation utilizing previously completed control assessment and aggregating the outcomes.

Organizations may develop a single, consolidated security and privacy assessment plan for the system or maintain separate plans. A consolidated assessment plan clearly delineates the roles and responsibilities for control assessment. If multiple organizations participate in assessing a system, a coordinated approach can reduce redundancies and associated costs.

Organizations can use other types of assessment activities, such as vulnerability scanning and system monitoring, to maintain the security and privacy posture of systems during the system life cycle. Assessment reports document assessment results in sufficient detail, as deemed necessary by organizations, to determine the accuracy and completeness of the reports and whether the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting requirements. Assessment results are provided to the individuals or roles appropriate for the types of assessments being conducted. For example, assessments conducted in support of authorization decisions are provided to authorizing officials, senior agency officials for privacy, senior agency information security officers, and authorizing official designated representatives.

To satisfy annual assessment requirements, organizations can use assessment results from the following sources: initial or ongoing system authorizations, continuous monitoring, systems engineering processes, or system development life cycle activities. Organizations ensure that assessment results are current, relevant to the determination of control effectiveness, and obtained with the appropriate level of assessor independence. Existing control assessment results can be reused to the extent that the results are still valid and can also be supplemented with additional assessments as needed. After the initial authorizations, organizations assess controls during continuous monitoring. Organizations also establish the frequency for ongoing assessments in accordance with organizational continuous monitoring strategies. External audits, including audits by external entities such as regulatory agencies, are outside of the scope of CA-2.

Control Assessments | Independent Assessors (CA-2(1))

Description for Control Assessments | Independent Assessors (CA-2(1))
Employ independent assessors or assessment teams to conduct control assessments.

Discussion for Control Assessments | Independent Assessors (CA-2(1))
Independent assessors or assessment teams are individuals or groups who conduct impartial assessments of systems. Impartiality means that assessors are free from any perceived or actual conflicts of interest regarding the development, operation, sustainment, or management of the systems under assessment or the determination of control effectiveness. To achieve impartiality, assessors do not create a mutual or conflicting interest with the organizations where the assessments are being conducted, assess their own work, act as management or employees of the organizations they are serving, or place themselves in positions of advocacy for the organizations acquiring their services.
Independent assessments can be obtained from elements within organizations or be contracted to public or private sector entities outside of organizations. Authorizing officials determine the required level of independence based on the security categories of systems and/or the risk to organizational operations, organizational assets, or individuals. Authorizing officials also determine if the level of assessor independence provides sufficient assurance that the results are sound and can be used to make credible, risk-based decisions. Assessor independence determination includes whether contracted assessment services have sufficient independence, such as when system owners are not directly involved in contracting processes or cannot influence the impartiality of the assessors conducting the assessments. During the system design and development phase, having independent assessors is analogous to having independent SMEs involved in design reviews.
When organizations that own the systems are small or the structures of the organizations require that assessments be conducted by individuals that are in the developmental, operational, or management chain of the system owners, independence in assessment processes can be achieved by ensuring that assessment results are carefully reviewed and analyzed by independent teams of experts to validate the completeness, accuracy, integrity, and reliability of the results. Assessments performed for purposes other than to support authorization decisions are more likely to be useable for such decisions when performed by assessors with sufficient independence, thereby reducing the need to repeat assessments.

Control Assessments | Specialized Assessments (CA-2(2))

Description for Control Assessments | Specialized Assessments (CA-2(2))
Include as part of control assessments, [Assignment: organization-defined frequency], [Selection: announced; unannounced], [Selection (one or more): in-depth monitoring; security instrumentation; automated security test cases; vulnerability scanning; malicious user testing; insider threat assessment; performance and load testing; data leakage or data loss assessment; [Assignment: organization-defined other forms of assessment]].

Discussion for Control Assessments | Specialized Assessments (CA-2(2))
Organizations can conduct specialized assessments, including verification and validation, system monitoring, insider threat assessments, malicious user testing, and other forms of testing. These assessments can improve readiness by exercising organizational capabilities and indicating current levels of performance as a means of focusing actions to improve security and privacy. Organizations conduct specialized assessments in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Authorizing officials approve the assessment methods in coordination with the organizational risk executive function. Organizations can include vulnerabilities uncovered during assessments into vulnerability remediation processes. Specialized assessments can also be conducted early in the system development life cycle (e.g., during initial design, development, and unit testing).

Control Assessments | Leveraging Results from External Organizations (CA-2(3))

Description for Control Assessments | Leveraging Results from External Organizations (CA-2(3))
Leverage the results of control assessments performed by [Assignment: organization-defined external organization] on [Assignment: organization-defined system] when the assessment meets [Assignment: organization-defined requirements].

Discussion for Control Assessments | Leveraging Results from External Organizations (CA-2(3))
Organizations may rely on control assessments of organizational systems by other (external) organizations. Using such assessments and reusing existing assessment evidence can decrease the time and resources required for assessments by limiting the independent assessment activities that organizations need to perform. The factors that organizations consider in determining whether to accept assessment results from external organizations can vary. Such factors include the organization's past experience with the organization that conducted the assessment, the reputation of the assessment organization, the level of detail of supporting assessment evidence provided, and mandates imposed by applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Accredited testing laboratories that support the Common Criteria Program ISO 15408-1, the NIST Cryptographic Module Validation Program (CMVP), or the NIST Cryptographic Algorithm Validation Program (CAVP) can provide independent assessment results that organizations can leverage.

Information Exchange (CA-3)

Description for Information Exchange (CA-3)
a. Approve and manage the exchange of information between the system and other systems using [Selection (one or more): interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service level agreements; user agreements; nondisclosure agreements; [Assignment: organization-defined type of agreement]];
b. Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated; and
c. Review and update the agreements [Assignment: organization-defined frequency].

Discussion for Information Exchange (CA-3)
System information exchange requirements apply to information exchanges between two or more systems. System information exchanges include connections via leased lines or virtual private networks, connections to internet service providers, database sharing or exchanges of database transaction information, connections and exchanges with cloud services, exchanges via web-based services, or exchanges of files via file transfer protocols, network protocols (e.g., IPv4, IPv6), email, or other organization-to-organization communications. Organizations consider the risk related to new or increased threats that may be introduced when systems 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.
Authorizing officials determine the risk associated with system information exchange and the controls needed for appropriate risk mitigation. The types of agreements selected are based on factors such as the impact level of the information being exchanged, the relationship between the organizations exchanging information (e.g., government to government, government to business, business to business, government or business to service provider, government or business to individual), or the level of access to the organizational system by users of the other system. If systems that exchange information have the same authorizing official, organizations need not develop agreements. Instead, the interface characteristics between the systems (e.g., how the information is being exchanged. how the information is protected) are described in the respective security and privacy plans. If the systems that exchange information have different authorizing officials within the same organization, the organizations can develop agreements or provide the same information that would be provided in the appropriate agreement type from CA-3a in the respective security and

privacy plans for the systems. Organizations may incorporate agreement information into formal contracts, especially for information exchanges established between federal agencies and nonfederal organizations (including service providers, contractors, system developers, and system integrators). Risk considerations include systems that share the same networks.

Information Exchange | Unclassified National Security System Connections (CA-3(1))

Description for Information Exchange | Unclassified National Security System Connections (CA-3(1))
[Withdrawn: Moved to SC-7(25).]

Discussion for Information Exchange | Unclassified National Security System Connections (CA-3(1))

Information Exchange | Classified National Security System Connections (CA-3(2))

Description for Information Exchange | Classified National Security System Connections (CA-3(2))
[Withdrawn: Moved to SC-7(26).]

Discussion for Information Exchange | Classified National Security System Connections (CA-3(2))

Information Exchange | Unclassified Non-national Security System Connections (CA-3(3))

Description for Information Exchange | Unclassified Non-national Security System Connections (CA-3(3))
[Withdrawn: Moved to SC-7(27).]

Discussion for Information Exchange | Unclassified Non-national Security System Connections (CA-3(3))

Information Exchange | Connections to Public Networks (CA-3(4))

Description for Information Exchange | Connections to Public Networks (CA-3(4))
[Withdrawn: Moved to SC-7(28).]

Discussion for Information Exchange | Connections to Public Networks (CA-3(4))

Information Exchange | Restrictions on External System Connections (CA-3(5))

Description for Information Exchange | Restrictions on External System Connections (CA-3(5))
[Withdrawn: Moved to SC-7(5).]

Discussion for Information Exchange | Restrictions on External System Connections (CA-3(5))

Information Exchange | Transfer Authorizations (CA-3(6))

Description for Information Exchange | Transfer Authorizations (CA-3(6))
Verify that individuals or systems transferring data between interconnecting systems have the requisite authorizations (i.e., write permissions or privileges) prior to accepting such data.

Discussion for Information Exchange | Transfer Authorizations (CA-3(6))
To prevent unauthorized individuals and systems from making information transfers to protected systems, the protected system verifies—via independent means— whether the individual or system attempting to transfer information is authorized to do so. Verification of the authorization to transfer information also

applies to control plane traffic (e.g., routing and DNS) and services (e.g., authenticated SMTP relays).

Information Exchange | Transitive Information Exchanges (CA-3(7))

Description for Information Exchange | Transitive Information Exchanges (CA-3(7))
(a) Identify transitive (downstream) information exchanges with other systems through the systems identified in CA-3a; and
(b) Take measures to ensure that transitive (downstream) information exchanges cease when the controls on identified transitive (downstream) systems cannot be verified or validated.

Discussion for Information Exchange | Transitive Information Exchanges (CA-3(7))
Transitive or downstream information exchanges are information exchanges between the system or systems with which the organizational system exchanges information and other systems. For mission-essential systems, services, and applications, including high value assets, it is necessary to identify such information exchanges. The transparency of the controls or protection measures in place in such downstream systems connected directly or indirectly to organizational systems is essential to understanding the security and privacy risks resulting from those information exchanges. Organizational systems can inherit risk from downstream systems through transitive connections and information exchanges, which can make the organizational systems more susceptible to threats, hazards, and adverse impacts.

Security Certification (CA-4)

Description for Security Certification (CA-4)
[Withdrawn: Incorporated into CA-2.]

Discussion for Security Certification (CA-4)

Plan of Action and Milestones (CA-5)

Description for Plan of Action and Milestones (CA-5)
a. Develop a plan of action and milestones for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and
b. Update existing plan of action and milestones [Assignment: organization-defined frequency] based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities.

Discussion for Plan of Action and Milestones (CA-5)
Plans of action and milestones are useful for any type of organization to track planned remedial actions. Plans of action and milestones are required in authorization packages and subject to federal reporting requirements established by OMB.

Plan of Action and Milestones | Automation Support for Accuracy and Currency (CA-5(1))

Description for Plan of Action and Milestones | Automation Support for Accuracy and Currency (CA-5(1))
Ensure the accuracy, currency, and availability of the plan of action and milestones for the system using [Assignment: organization-defined automated mechanisms].

Discussion for Plan of Action and Milestones | Automation Support for Accuracy and Currency (CA-5(1))
Using automated tools helps maintain the accuracy, currency, and availability of the plan of action and milestones and facilitates the coordination and sharing of security and privacy information throughout the organization. Such coordination and information sharing help to identify systemic weaknesses or deficiencies in organizational systems and ensure that appropriate resources are directed at the most critical system vulnerabilities in a timely manner.

Authorization (CA-6)

Description for Authorization (CA-6)
a. Assign a senior official as the authorizing official for the system;
b. Assign a senior official as the authorizing official for common controls available for inheritance by organizational systems;
c. Ensure that the authorizing official for the system, before commencing operations:
1. Accepts the use of common controls inherited by the system; and
2. Authorizes the system to operate;
d. Ensure that the authorizing official for common controls authorizes the use of those controls for inheritance by organizational systems;
e. Update the authorizations [Assignment: organization-defined frequency].

Discussion for Authorization (CA-6)
Authorizations are official management decisions by senior officials to authorize operation of systems, authorize the use of common controls for inheritance by organizational systems, and 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 common controls or assume responsibility for the mission and business functions supported by those 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. Nonfederal organizations may have similar processes to authorize systems and senior officials that assume the authorization role and associated responsibilities.

Authorizing officials issue ongoing authorizations of systems based on evidence produced from implemented continuous monitoring programs. Robust continuous monitoring programs reduce the need for separate reauthorization processes. Through the employment of comprehensive continuous monitoring processes, the information contained in authorization packages (i.e., security and privacy plans, assessment reports, and plans of action and milestones) is updated on an ongoing basis. This provides authorizing officials, common control providers, and system owners with an up-to-date status of the security and privacy posture of their systems, controls, and operating environments. To reduce the cost of reauthorization, authorizing officials can leverage the results of continuous monitoring processes to the maximum extent possible as the basis for rendering reauthorization decisions.

Authorization | Joint Authorization — Intra-organization (CA-6(1))

Description for Authorization | Joint Authorization — Intra-organization (CA-6(1))
Employ a joint authorization process for the system that includes multiple authorizing officials from the same organization conducting the authorization.

Discussion for Authorization | Joint Authorization — Intra-organization (CA-6(1))
Assigning multiple authorizing officials from the same organization to serve as co-authorizing officials for the system increases the level of independence in the risk-based decision-making process. It also implements the concepts of separation of duties and dual authorization as applied to the system authorization process. The intra-organization joint authorization process is most relevant for connected systems, shared systems, and systems with multiple information owners.

Authorization | Joint Authorization — Inter-organization (CA-6(2))

Description for Authorization | Joint Authorization — Inter-organization (CA-6(2))
Employ a joint authorization process for the system that includes multiple authorizing officials with at least one authorizing official from an organization external to the organization conducting the authorization.

Discussion for Authorization | Joint Authorization — Inter-organization (CA-6(2))
Assigning multiple authorizing officials, at least one of whom comes from an external organization, to serve as co-authorizing officials for the system increases the level of independence in the risk-based decision-making process. It implements the concepts of separation of duties and dual authorization as applied to the system authorization process. Employing authorizing officials from external organizations to supplement the authorizing official from the organization that owns or hosts the system may be necessary when the external organizations have a vested interest or equities in the outcome of the authorization decision. The inter-organization joint authorization process is relevant and appropriate for connected systems, shared systems or services, and systems with multiple information owners. The authorizing officials from the external organizations are key stakeholders of the system undergoing authorization.

Continuous Monitoring (CA-7)

Description for Continuous Monitoring (CA-7)
Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes:
a. Establishing the following system-level metrics to be monitored: [Assignment: organization-defined system-level metrics];
b. Establishing [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessment of control effectiveness;
c. Ongoing control assessments in accordance with the continuous monitoring strategy;
d. Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy;
e. Correlation and analysis of information generated by control assessments and monitoring;
f. Response actions to address results of the analysis of control assessment and monitoring information; and
g. Reporting the security and privacy status of the system to [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency].

Discussion for Continuous Monitoring (CA-7)
Continuous monitoring at the system level facilitates ongoing awareness of the system security and privacy posture to support organizational risk management decisions. The terms continuous and ongoing imply that organizations assess and monitor their controls and risks at a frequency sufficient to support risk-based decisions. Different types of controls may require different monitoring frequencies. The results of continuous monitoring generate risk response actions by organizations. When monitoring the effectiveness of multiple controls that have been grouped into capabilities, a root-cause analysis may be needed to determine the specific control that has failed. Continuous monitoring programs allow organizations to maintain the authorizations of systems and common controls in highly dynamic environments of operation with changing mission and business needs, threats, vulnerabilities, and technologies. Having access to security and privacy information on a continuing basis through reports and dashboards gives organizational officials the ability to make effective and timely risk management decisions, including ongoing authorization decisions.
Automation 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, such as 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, MA-4a, PE-3d, PE-6, PE-14b, PE-16, PE-20, PM-6, PM-23, PM-31, PS-7e, SA-9c, SR-4, SC-5(3)(b), SC-7a, SC-7(24)(b), SC-18b, SC-43b, and SI-4.

Continuous Monitoring | Independent Assessment (CA-7(1))

Description for Continuous Monitoring | Independent Assessment (CA-7(1))
Employ independent assessors or assessment teams to monitor the controls in the system on an ongoing basis.

Discussion for Continuous Monitoring | Independent Assessment (CA-7(1))
Organizations maximize the value of control assessments by requiring that assessments be conducted by assessors with appropriate levels of independence. The level of required independence is based on organizational continuous monitoring strategies. Assessor independence provides a degree of impartiality to the monitoring process. To achieve such impartiality, assessors do not create a mutual or conflicting interest with the organizations where the assessments are being conducted, assess their own work, act as management or employees of the organizations they are serving, or place themselves in advocacy positions for the organizations acquiring their services.

Continuous Monitoring | Types of Assessments (CA-7(2))

Description for Continuous Monitoring | Types of Assessments (CA-7(2))
[Withdrawn: Incorporated into CA-2.]

Discussion for Continuous Monitoring | Types of Assessments (CA-7(2))

Continuous Monitoring | Trend Analyses (CA-7(3))

Description for Continuous Monitoring | Trend Analyses (CA-7(3))
Employ trend analyses to determine if control implementations, the frequency of continuous monitoring activities, and the types of activities used in the continuous monitoring process need to be modified based on empirical data.

Discussion for Continuous Monitoring | Trend Analyses (CA-7(3))
Trend analyses include examining recent threat information that addresses the types of threat events that have occurred in the organization or the Federal Government, success rates of certain types of attacks, emerging vulnerabilities in technologies, evolving social engineering techniques, the effectiveness of configuration settings, results from multiple control assessments, and findings from Inspectors General or auditors.

Continuous Monitoring | Risk Monitoring (CA-7(4))

Description for Continuous Monitoring | Risk Monitoring (CA-7(4))
Ensure risk monitoring is an integral part of the continuous monitoring strategy that includes the following:
(a) Effectiveness monitoring;
(b) Compliance monitoring; and
(c) Change monitoring.

Discussion for Continuous Monitoring | Risk Monitoring (CA-7(4))
Risk monitoring is informed by the established organizational risk tolerance. Effectiveness monitoring determines the ongoing effectiveness of the implemented risk response measures. Compliance monitoring verifies that required risk response measures are implemented. It also verifies that security and privacy requirements are satisfied. Change monitoring identifies changes to organizational systems and environments of operation that may affect security and privacy risk.

Continuous Monitoring | Consistency Analysis (CA-7(5))

Description for Continuous Monitoring | Consistency Analysis (CA-7(5))
Employ the following actions to validate that policies are established and implemented controls are operating in a consistent manner: [Assignment: organization-defined actions].

Discussion for Continuous Monitoring | Consistency Analysis (CA-7(5))
Security and privacy controls are often added incrementally to a system. As a result, policies for selecting and implementing controls may be inconsistent, and the controls could fail to work together in a consistent or coordinated manner. At a minimum, the lack of consistency and coordination could mean that there are unacceptable security and privacy gaps in the system. At worst, it could mean that some of the controls implemented in one location or by one component are actually impeding the functionality of other controls (e.g., encrypting internal network traffic can impede monitoring). In other situations, failing to consistently monitor all implemented network protocols (e.g., a dual stack of IPv4 and IPv6) may create unintended vulnerabilities in the system that could be exploited by adversaries. It is important to validate—through testing, monitoring, and analysis—that the implemented controls are operating in a consistent, coordinated, non-interfering manner.

Continuous Monitoring | Automation Support for Monitoring (CA-7(6))

Description for Continuous Monitoring | Automation Support for Monitoring (CA-7(6))
Ensure the accuracy, currency, and availability of monitoring results for the system using [Assignment: organization-defined automated mechanisms].

Discussion for Continuous Monitoring | Automation Support for Monitoring (CA-7(6))
Using automated tools for monitoring helps to maintain the accuracy, currency, and availability of monitoring information which in turns helps to increase the level of ongoing awareness of the system security and privacy posture in support of organizational risk management decisions.

Penetration Testing (CA-8)

Description for Penetration Testing (CA-8)
Conduct penetration testing [Assignment: organization-defined frequency] on [Assignment: organization-defined systems or system components].

Discussion for Penetration Testing (CA-8)
Penetration testing is a specialized type of assessment conducted on systems or individual system components to identify vulnerabilities that could be exploited by adversaries. Penetration testing goes beyond automated vulnerability scanning and is conducted by agents and teams with demonstrable skills and experience that include technical expertise in network, operating system, and/or application level security. Penetration testing can be used to validate vulnerabilities or determine the degree of penetration resistance of systems to adversaries within specified constraints. Such constraints include time, resources, and skills. Penetration testing attempts to duplicate the actions of adversaries and provides a more in-depth analysis of security- and privacy-related weaknesses or deficiencies. Penetration testing is especially important when organizations are transitioning from older technologies to newer technologies (e.g., transitioning from IPv4 to IPv6 network protocols).
Organizations can use the results of vulnerability analyses to support penetration testing activities. Penetration testing can be conducted internally or externally on the hardware, software, or firmware components of a system and can exercise both physical and technical controls. A standard method for penetration testing includes a pretest analysis based on full knowledge of the system, pretest identification of potential vulnerabilities based on the pretest analysis, and testing designed to determine the exploitability of vulnerabilities. All parties agree to the rules of engagement before commencing penetration testing scenarios. Organizations correlate the rules of engagement for the penetration tests with the tools, techniques, and procedures that are anticipated to be employed by adversaries. Penetration testing may result in the exposure of information that is protected by laws or regulations, to individuals conducting the testing. Rules of engagement, contracts, or other appropriate mechanisms can be used to communicate expectations for how to protect this information. Risk assessments guide the decisions on the level of independence required for the personnel conducting penetration testing.

Penetration Testing | Independent Penetration Testing Agent or Team (CA-8(1))

Description for Penetration Testing | Independent Penetration Testing Agent or Team (CA-8(1))
Employ an independent penetration testing agent or team to perform penetration testing on the system or system components.

Discussion for Penetration Testing | Independent Penetration Testing Agent or Team (CA-8(1))
Independent penetration testing agents or teams are individuals or groups who conduct impartial penetration testing of organizational systems. Impartiality implies that penetration testing agents or teams are free from perceived or actual conflicts of interest with respect to the development, operation, or management of the systems that are the targets of the penetration testing. CA-2(1) provides additional information on independent assessments that can be applied to penetration testing.

Penetration Testing | Red Team Exercises (CA-8(2))

Description for Penetration Testing | Red Team Exercises (CA-8(2))
Employ the following red-team exercises to simulate attempts by adversaries to compromise organizational systems in accordance with applicable rules of engagement: [Assignment: organization-defined red team exercises].

Discussion for Penetration Testing | Red Team Exercises (CA-8(2))
Red team exercises extend the objectives of penetration testing by examining the security and privacy posture of organizations and the capability to implement effective cyber defenses. Red team exercises simulate attempts by adversaries to compromise mission and business functions and provide a comprehensive assessment of the security and privacy posture of systems and organizations. Such attempts may include technology-based attacks and social engineering-based attacks. Technology-based attacks include interactions with hardware, software, or firmware components and/or mission and business processes. Social engineering-based attacks include interactions via email, telephone, shoulder surfing, or personal conversations. Red team exercises are most effective when conducted by penetration testing agents and teams with knowledge of and experience with current adversarial tactics, techniques, procedures, and tools. While penetration testing may be primarily laboratory-based testing, organizations can use red team exercises to provide more comprehensive assessments that reflect real-world conditions. The results from red team exercises can be used by organizations to improve security and privacy awareness and training and to assess control effectiveness.

Penetration Testing | Facility Penetration Testing (CA-8(3))

Description for Penetration Testing | Facility Penetration Testing (CA-8(3))
Employ a penetration testing process that includes [Assignment: organization-defined frequency] [Selection: announced; unannounced] attempts to bypass or circumvent controls associated with physical access points to the facility.

Discussion for Penetration Testing | Facility Penetration Testing (CA-8(3))
Penetration testing of physical access points can provide information on critical vulnerabilities in the operating environments of organizational systems. Such information can be used to correct weaknesses or deficiencies in physical controls that are necessary to protect organizational systems.

Internal System Connections (CA-9)

Description for Internal System Connections (CA-9)
a. Authorize internal connections of [Assignment: organization-defined system components or classes of components] to the system;
b. Document, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated;
c. Terminate internal system connections after [Assignment: organization-defined conditions]; and
d. Review [Assignment: organization-defined frequency] the continued need for each internal connection.

Discussion for Internal System Connections (CA-9)
Internal system connections are connections between organizational systems and separate constituent system components (i.e., connections between components that are part of the same system) including components used for system development. Intra-system connections include connections with mobile devices, notebook and desktop computers, tablets, printers, copiers, facsimile machines, scanners, sensors, and servers. Instead of authorizing each internal system connection individually, organizations can authorize internal connections for a class of system components with common characteristics and/or configurations, including printers, scanners, and copiers with a specified processing, transmission, and storage capability or smart phones and tablets with a specific baseline configuration. The continued need for an internal system connection is reviewed from the perspective of whether it provides support for organizational missions or business functions.

Internal System Connections | Compliance Checks (CA-9(1))

Description for Internal System Connections | Compliance Checks (CA-9(1))
Perform security and privacy compliance checks on constituent system components prior to the establishment of the internal connection.

Discussion for Internal System Connections | Compliance Checks (CA-9(1))
Compliance checks include verification of the relevant baseline configuration.

Policy and Procedures (CM-1)

Description for Policy and Procedures (CM-1)
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] configuration management policy that:
(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the configuration management policy and the associated configuration management controls;
b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the configuration management policy and procedures; and
c. Review and update the current configuration management:
1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

Discussion for Policy and Procedures (CM-1)
Configuration management policy and procedures address the controls in the CM family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of configuration management policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission/business processes, 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. Events that may precipitate an update to configuration management policy and procedures include, but are not limited to, assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Baseline Configuration (CM-2)

Description for Baseline Configuration (CM-2)
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:
1. [Assignment: organization-defined frequency];
2. When required due to [Assignment: organization-defined circumstances]; and
3. When system components are installed or upgraded.

Discussion for Baseline Configuration (CM-2)
Baseline configurations for systems and system components include connectivity, operational, and communications aspects of systems. Baseline configurations are documented, formally reviewed, and agreed-upon specifications for systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, or changes to systems and include security and privacy control implementations, operational procedures, information about system components, network topology, 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.

User-installed Software | Alerts for Unauthorized Installations (CM-11(1))

Description for User-installed Software | Alerts for Unauthorized Installations (CM-11(1))
[Withdrawn: Incorporated into CM-8(3).]

Discussion for User-installed Software | Alerts for Unauthorized Installations (CM-11(1))

Baseline Configuration | Automation Support for Accuracy and Currency (CM-2(2))

Description for Baseline Configuration | Automation Support for Accuracy and Currency (CM-2(2))
Maintain the currency, completeness, accuracy, and availability of the baseline configuration of the system using [Assignment: organization-defined automated mechanisms].

Discussion for Baseline Configuration | Automation Support for Accuracy and Currency (CM-2(2))
Automated mechanisms that help organizations maintain consistent baseline configurations for systems include configuration management tools, hardware, software, firmware inventory tools, and network management tools. Automated tools can be used at the organization level, mission and business process level, or system level on workstations, servers, notebook computers, network components, or mobile devices. Tools can be used to track version numbers on operating systems, applications, types of software installed, and current patch levels. Automation support for accuracy and currency can be satisfied by the implementation of CM-8(2) for organizations that combine system component inventory and baseline configuration activities.

Baseline Configuration | Retention of Previous Configurations (CM-2(3))

Description for Baseline Configuration | Retention of Previous Configurations (CM-2(3))
Retain [Assignment: organization-defined number] of previous versions of baseline configurations of the system to support rollback.

Discussion for Baseline Configuration | Retention of Previous Configurations (CM-2(3))
Retaining previous versions of baseline configurations to support rollback include hardware, software, firmware, configuration files, configuration records, and associated documentation.

Baseline Configuration | Reviews and Updates (CM-2(1))

Description for Baseline Configuration | Reviews and Updates (CM-2(1))
[Withdrawn: Incorporated into CM-2.]

Discussion for Baseline Configuration | Reviews and Updates (CM-2(1))

Baseline Configuration | Unauthorized Software (CM-2(4))

Description for Baseline Configuration | Unauthorized Software (CM-2(4))
[Withdrawn: Incorporated into CM-7(4).]

Discussion for Baseline Configuration | Unauthorized Software (CM-2(4))

Baseline Configuration | Development and Test Environments (CM-2(6))

Description for Baseline Configuration | Development and Test Environments (CM-2(6))
Maintain a baseline configuration for system development and test environments that is managed separately from the operational baseline configuration.

Discussion for Baseline Configuration | Development and Test Environments (CM-2(6))
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 stability, 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.

Baseline Configuration | Configure Systems and Components for High-risk Areas (CM-2(7))

Description for Baseline Configuration | Configure Systems and Components for High-risk Areas (CM-2(7))
(a) Issue [Assignment: organization-defined systems or system components] with [Assignment: organization-defined configurations] to individuals traveling to locations that the organization deems to be of significant risk; and
(b) Apply the following controls to the systems or components when the individuals return from travel: [Assignment: organization-defined controls].

Discussion for Baseline Configuration | Configure Systems and Components for High-risk Areas (CM-2(7))
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 that are of concern, defining the required configurations for the components, ensuring that components are configured as intended before travel is initiated, and applying controls to the components after travel is completed. Specially configured notebook computers include computers with sanitized hard drives, limited applications, and more stringent configuration settings. Controls applied to mobile devices upon return from travel include examining the mobile device for signs of physical tampering and purging and reimaging disk drives. Protecting information that resides on mobile devices is addressed in the MP (Media Protection) family.

Configuration Change Control (CM-3)

Description for Configuration Change Control (CM-3)
a. Determine and document the types of changes to the system that are configuration-controlled;
b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses;
c. Document configuration change decisions associated with the system;
d. Implement approved configuration-controlled changes to the system;
e. Retain records of configuration-controlled changes to the system for [Assignment: organization-defined time period];
f. Monitor and review activities associated with configuration-controlled changes to the system; and
g. Coordinate and provide oversight for configuration change control activities through [Assignment: organization-defined configuration change control element] that convenes [Selection (one or more): [Assignment: organization-defined frequency]; when [Assignment: organization-defined configuration change conditions]].

Discussion for Configuration Change Control (CM-3)
Configuration change control for organizational systems involves the systematic proposal, justification, implementation, testing, review, and disposition of system changes, including system upgrades and modifications. Configuration change control includes changes to baseline configurations, configuration items of systems, operational procedures, configuration settings for system components, remediate vulnerabilities, and unscheduled or unauthorized changes. Processes for managing configuration changes to systems include Configuration Control Boards or Change Advisory Boards that review and approve proposed changes. For changes that impact privacy risk, the senior agency official for privacy updates privacy impact assessments and system of records notices. For new systems or major upgrades, organizations consider including representatives from the development organizations on the Configuration Control Boards or Change Advisory Boards. Auditing of changes includes activities before and after changes are made to systems and the auditing activities required to implement such changes. See also SA-10.

Configuration Change Control | Automated Documentation, Notification, and Prohibition of Changes (CM-3(1))

Description for Configuration Change Control | Automated Documentation, Notification, and Prohibition of Changes (CM-3(1))
Use [Assignment: organization-defined automated mechanisms] to:
(a) Document proposed changes to the system;
(b) Notify [Assignment: organization-defined approval authorities] of proposed changes to the system and request change approval;
(c) Highlight proposed changes to the system that have not been approved or disapproved within [Assignment: organization-defined time period];
(d) Prohibit changes to the system until designated approvals are received;
(e) Document all changes to the system; and
(f) Notify [Assignment: organization-defined personnel] when approved changes to the system are completed.

Discussion for Configuration Change Control | Automated Documentation, Notification, and Prohibition of Changes (CM-3(1))
None.

Configuration Change Control | Testing, Validation, and Documentation of Changes (CM-3(2))

Description for Configuration Change Control | Testing, Validation, and Documentation of Changes (CM-3(2))
Test, validate, and document changes to the system before finalizing the implementation of the changes.

Discussion for Configuration Change Control | Testing, Validation, and Documentation of Changes (CM-3(2))
Changes to systems include modifications to hardware, software, or firmware components and configuration settings defined in CM-6. Organizations ensure that testing does not interfere with system operations that support organizational mission and business functions. Individuals or groups conducting tests understand security and privacy policies and procedures, system security and privacy policies and procedures, and the health, safety, and environmental risks associated with

specific facilities or processes. Operational systems may need to be taken offline, or replicated to the extent feasible, before testing can be conducted. If systems must be taken offline for testing, the tests are scheduled to occur during planned system outages whenever possible. If the testing cannot be conducted on operational systems, organizations employ compensating controls.

Configuration Change Control | Automated Change Implementation (CM-3(3))

Description for Configuration Change Control | Automated Change Implementation (CM-3(3))
Implement changes to the current system baseline and deploy the updated baseline across the installed base using [Assignment: organization-defined automated mechanisms].

Discussion for Configuration Change Control | Automated Change Implementation (CM-3(3))
Automated tools can improve the accuracy, consistency, and availability of configuration baseline information. Automation can also provide data aggregation and data correlation capabilities, alerting mechanisms, and dashboards to support risk-based decision-making within the organization.

Configuration Change Control | Security and Privacy Representatives (CM-3(4))

Description for Configuration Change Control | Security and Privacy Representatives (CM-3(4))
Require [Assignment: organization-defined security and privacy representatives] to be members of the [Assignment: organization-defined configuration change control element].

Discussion for Configuration Change Control | Security and Privacy Representatives (CM-3(4))
Information security and privacy representatives include system security officers, senior agency information security officers, senior agency officials for privacy, or system privacy officers. Representation by personnel with information security and privacy expertise is important because changes to system configurations can have unintended side effects, some of which may be security- or privacy-relevant. Detecting such changes early in the process can help avoid unintended, negative consequences that could ultimately affect the security and privacy posture of systems. The configuration change control element referred to in the second organization-defined parameter reflects the change control elements defined by organizations in CM-3g.

Configuration Change Control | Automated Security Response (CM-3(5))

Description for Configuration Change Control | Automated Security Response (CM-3(5))
Implement the following security responses automatically if baseline configurations are changed in an unauthorized manner: [Assignment: organization-defined security responses].

Discussion for Configuration Change Control | Automated Security Response (CM-3(5))
Automated security responses include halting selected system functions, halting system processing, and issuing alerts or notifications to organizational personnel when there is an unauthorized modification of a configuration item.

Configuration Change Control | Cryptography Management (CM-3(6))

Description for Configuration Change Control | Cryptography Management (CM-3(6))
Ensure that cryptographic mechanisms used to provide the following controls are under configuration management: [Assignment: organization-defined controls].

Discussion for Configuration Change Control | Cryptography Management (CM-3(6))
The controls referenced in the control enhancement 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 use certificates for identification and authentication, a process is implemented to address the expiration of those certificates.

Configuration Change Control | Review System Changes (CM-3(7))

Description for Configuration Change Control | Review System Changes (CM-3(7))
Review changes to the system [Assignment: organization-defined frequency] or when [Assignment: organization-defined circumstances] to determine whether unauthorized changes have occurred.

Discussion for Configuration Change Control | Review System Changes (CM-3(7))
Indications that warrant a review of changes to the system and the specific circumstances justifying such reviews may be obtained from activities carried out by organizations during the configuration change process or continuous monitoring process.

Configuration Change Control | Prevent or Restrict Configuration Changes (CM-3(8))

Description for Configuration Change Control | Prevent or Restrict Configuration Changes (CM-3(8))
Prevent or restrict changes to the configuration of the system under the following circumstances: [Assignment: organization-defined circumstances].

Discussion for Configuration Change Control | Prevent or Restrict Configuration Changes (CM-3(8))
System configuration changes can adversely affect critical system security and privacy functionality. Change restrictions can be enforced through automated mechanisms.

Impact Analyses (CM-4)

Description for Impact Analyses (CM-4)
Analyze changes to the system to determine potential security and privacy impacts prior to change implementation.

Discussion for Impact Analyses (CM-4)
Organizational personnel with security or privacy responsibilities conduct impact analyses. Individuals conducting impact analyses possess the necessary skills and technical expertise to analyze the changes to systems as well as the security or privacy ramifications. Impact analyses include reviewing security and privacy plans, policies, and procedures to understand control requirements; reviewing system design documentation and operational procedures to understand control implementation and how specific system changes might affect the controls; reviewing the impact of changes on organizational supply chain partners with stakeholders; and determining how potential changes to a system create new risks to the 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 determine if additional controls are required.

Impact Analyses | Separate Test Environments (CM-4(1))

Description for Impact Analyses | Separate Test Environments (CM-4(1))
Analyze 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.

Discussion for Impact Analyses | Separate Test Environments (CM-4(1))
A separate test environment requires an environment that is physically or logically separate and distinct from the operational environment. The separation is sufficient to ensure that activities in the test environment do not impact activities in the operational environment and that information in the operational environment is not inadvertently transmitted to the test environment. Separate environments can be achieved by physical or logical means. If physically separate test environments are not implemented, organizations determine the strength of mechanism required when implementing logical separation.

Impact Analyses | Verification of Controls (CM-4(2))

Description for Impact Analyses | Verification of Controls (CM-4(2))
After system changes, verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security and privacy requirements for the system.

Discussion for Impact Analyses | Verification of Controls (CM-4(2))
Implementation in this context refers to installing changed code in the operational system that may have an impact on security or privacy controls.

Access Restrictions for Change (CM-5)

Description for Access Restrictions for Change (CM-5)
Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.

Discussion for Access Restrictions for Change (CM-5)
Changes to the hardware, software, or firmware components of systems or the operational procedures related to the system can potentially have significant effects on the security of the systems or individuals' privacy. Therefore, organizations permit only qualified and authorized individuals to access systems for purposes of initiating changes. Access restrictions include physical and logical access controls (see AC-3 and PE-3), software libraries, workflow automation, media libraries, abstract layers (i.e., changes implemented into external interfaces rather than directly into systems), and change windows (i.e., changes occur only during specified times).

Access Restrictions for Change | Automated Access Enforcement and Audit Records (CM-5(1))

Description for Access Restrictions for Change | Automated Access Enforcement and Audit Records (CM-5(1))
(a) Enforce access restrictions using [Assignment: organization-defined automated mechanisms]; and
(b) Automatically generate audit records of the enforcement actions.

Discussion for Access Restrictions for Change | Automated Access Enforcement and Audit Records (CM-5(1))
Organizations log system accesses associated with applying configuration changes to ensure that configuration change control is implemented and to support after-the-fact actions should organizations discover any unauthorized changes.

Baseline Configuration | Authorized Software (CM-2(5))

Description for Baseline Configuration | Authorized Software (CM-2(5))
[Withdrawn: Incorporated into CM-7(5).]

Discussion for Baseline Configuration | Authorized Software (CM-2(5))

Access Restrictions for Change | Review System Changes (CM-5(2))

Description for Access Restrictions for Change | Review System Changes (CM-5(2))
[Withdrawn: Incorporated into CM-3(7).]

Discussion for Access Restrictions for Change | Review System Changes (CM-5(2))

Access Restrictions for Change | Dual Authorization (CM-5(4))

Description for Access Restrictions for Change | Dual Authorization (CM-5(4))
Enforce dual authorization for implementing changes to [Assignment: organization-defined system components and system-level information].

Discussion for Access Restrictions for Change | Dual Authorization (CM-5(4))
Organizations employ dual authorization to help ensure that any changes to selected system components and information cannot occur unless two qualified individuals approve and implement such changes. The two individuals possess the skills and expertise to determine if the proposed changes are correct implementations of approved changes. The individuals are also accountable for the changes. 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. System-level information includes operational procedures.

Access Restrictions for Change | Privilege Limitation for Production and Operation (CM-5(5))

Description for Access Restrictions for Change | Privilege Limitation for Production and Operation (CM-5(5))
(a) Limit privileges to change system components and system-related information within a production or operational environment; and
(b) Review and reevaluate privileges [Assignment: organization-defined frequency].

Discussion for Access Restrictions for Change | Privilege Limitation for Production and Operation (CM-5(5))
In many organizations, systems support multiple mission and business functions. Limiting privileges to change system components with respect to operational systems is necessary because changes to a system component may have far-reaching effects on mission and business processes supported by the system. The relationships between systems and mission/business processes are, in some cases, unknown to developers. System-related information includes operational procedures.

Access Restrictions for Change | Limit Library Privileges (CM-5(6))

Description for Access Restrictions for Change | Limit Library Privileges (CM-5(6))
Limit privileges to change software resident within software libraries.

Discussion for Access Restrictions for Change | Limit Library Privileges (CM-5(6))
Software libraries include privileged programs.

Access Restrictions for Change | Signed Components (CM-5(3))

Description for Access Restrictions for Change | Signed Components (CM-5(3))
[Withdrawn: Moved to CM-14.]

Discussion for Access Restrictions for Change | Signed Components (CM-5(3))

Configuration Settings (CM-6)

Description for Configuration Settings (CM-6)
a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using [Assignment: organization-defined common secure configurations];
b. Implement the configuration settings;
c. Identify, document, and approve any deviations from established configuration settings for [Assignment: organization-defined system components] based on [Assignment: organization-defined operational requirements]; and
d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

Discussion for Configuration Settings (CM-6)
Configuration settings are the parameters that can be changed in the hardware, software, or firmware components of the system that affect the security and privacy posture or functionality of the system. Information technology products for which configuration settings can be defined include mainframe computers, servers, workstations, operating systems, mobile devices, input/output devices, protocols, and applications. Parameters that impact the security posture of systems include registry settings; account, file, or directory permission settings; and settings for functions, protocols, ports, services, and remote connections. Privacy parameters are parameters impacting the privacy posture of systems, including the parameters required to satisfy other privacy controls. Privacy parameters include settings for access controls, data processing preferences, and processing and retention permissions. Organizations establish organization-wide configuration settings and subsequently derive 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, lockdown and hardening guides, and security reference guides) provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for information technology products and platforms as well as instructions for configuring those products or platforms to meet operational requirements. Common secure configurations can be developed by a variety of organizations, including information technology product developers, manufacturers, vendors, federal agencies, consortia, academia, industry, and other organizations in the public and private sectors.
Implementation of a common secure configuration may be mandated at the

organization level, mission and business process level, system level, or at a higher level, including by a regulatory agency. Common secure configurations include the United States Government Configuration Baseline USGCB and security technical implementation guides (STIGs), which affect the implementation of CM-6 and other controls such as AC-19 and CM-7. The Security Content Automation Protocol (SCAP) and the defined standards within the protocol provide an effective method to uniquely identify, track, and control configuration settings.

Configuration Settings | Automated Management, Application, and Verification (CM-6(1))

Description for Configuration Settings | Automated Management, Application, and Verification (CM-6(1))
Manage, apply, and verify configuration settings for [Assignment: organization-defined system components] using [Assignment: organization-defined automated mechanisms].

Discussion for Configuration Settings | Automated Management, Application, and Verification (CM-6(1))
Automated tools (e.g., hardening tools, baseline configuration tools) can improve the accuracy, consistency, and availability of configuration settings information. Automation can also provide data aggregation and data correlation capabilities, alerting mechanisms, and dashboards to support risk-based decision-making within the organization.

Configuration Settings | Respond to Unauthorized Changes (CM-6(2))

Description for Configuration Settings | Respond to Unauthorized Changes (CM-6(2))
Take the following actions in response to unauthorized changes to [Assignment: organization-defined configuration settings]: [Assignment: organization-defined actions].

Discussion for Configuration Settings | Respond to Unauthorized Changes (CM-6(2))
Responses to unauthorized changes to configuration settings include alerting designated organizational personnel, restoring established configuration settings, or—in extreme cases—halting affected system processing.

Access Restrictions for Change | Automatic Implementation of Security Safeguards (CM-5(7))

Description for Access Restrictions for Change | Automatic Implementation of Security Safeguards (CM-5(7))
[Withdrawn: Incorporated into SI-7.]

Discussion for Access Restrictions for Change | Automatic Implementation of Security Safeguards (CM-5(7))

Configuration Settings | Unauthorized Change Detection (CM-6(3))

Description for Configuration Settings | Unauthorized Change Detection (CM-6(3))
[Withdrawn: Incorporated into SI-7.]

Discussion for Configuration Settings | Unauthorized Change Detection (CM-6(3))

Least Functionality (CM-7)

Description for Least Functionality (CM-7)
a. Configure the system to provide only [Assignment: organization-defined mission essential capabilities]; and
b. Prohibit or restrict the use of the following functions, ports, protocols, software, and/or services: [Assignment: organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services].

Discussion for Least Functionality (CM-7)
Systems provide a wide variety of functions and services. Some of the functions and services routinely provided by default may not be necessary to support essential organizational missions, functions, or operations. Additionally, it is sometimes convenient to provide multiple services from a single system component, but doing so increases risk over limiting the services provided by that single component. Where feasible, organizations limit component functionality to a single function per component. Organizations consider removing unused or unnecessary software and disabling unused or unnecessary physical and logical ports and protocols to prevent unauthorized connection of components, transfer of information, and tunneling. Organizations employ network scanning tools, intrusion detection and prevention systems, and end-point protection technologies, such as firewalls and host-based intrusion detection systems, to identify and prevent the use of prohibited functions, protocols, ports, and services. Least functionality can also be achieved as part of the fundamental design and development of the system (see SA-8, SC-2, and SC-3).

Least Functionality | Periodic Review (CM-7(1))

Description for Least Functionality | Periodic Review (CM-7(1))
(a) Review the system [Assignment: organization-defined frequency] to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services; and
(b) Disable or remove [Assignment: organization-defined functions, ports, protocols, software, and services within the system deemed to be unnecessary and/or nonsecure].

Discussion for Least Functionality | Periodic Review (CM-7(1))
Organizations review functions, ports, protocols, and services provided by systems or system components to determine the functions and services that are candidates for elimination. Such reviews are especially important during transition periods from older technologies to newer technologies (e.g., transition from IPv4 to IPv6). These technology transitions may require implementing the older and newer technologies simultaneously during the transition period and returning to minimum essential functions, ports, protocols, and services at the earliest opportunity. Organizations can either decide the relative security of the function, port, protocol, and/or service or base the security decision on the assessment of other entities. Unsecure protocols include Bluetooth, FTP, and peer-to-peer networking.

Least Functionality | Prevent Program Execution (CM-7(2))

Description for Least Functionality | Prevent Program Execution (CM-7(2))
Prevent program execution in accordance with [Selection (one or more): [Assignment: organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions]; rules authorizing the terms and conditions of software program usage].

Discussion for Least Functionality | Prevent Program Execution (CM-7(2))
Prevention of program execution addresses organizational policies, rules of behavior, and/or access agreements that restrict software usage and the terms and conditions imposed by the developer or manufacturer, including software licensing and copyrights. Restrictions include prohibiting auto-execute features, restricting roles allowed to approve program execution, permitting or prohibiting specific software programs, or restricting the number of program instances executed at the same time.

Least Functionality | Registration Compliance (CM-7(3))

Description for Least Functionality | Registration Compliance (CM-7(3))
Ensure compliance with [Assignment: organization-defined registration requirements for functions, ports, protocols, and services].

Discussion for Least Functionality | Registration Compliance (CM-7(3))
Organizations use the registration process to manage, track, and provide oversight for systems and implemented functions, ports, protocols, and services.

Least Functionality | Unauthorized Software — Deny-by-exception (CM-7(4))

Description for Least Functionality | Unauthorized Software — Deny-by-exception (CM-7(4))
(a) Identify [Assignment: organization-defined software programs not authorized to execute on the system];
(b) Employ an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the system; and
(c) Review and update the list of unauthorized software programs [Assignment: organization-defined frequency].

Discussion for Least Functionality | Unauthorized Software — Deny-by-exception (CM-7(4))
Unauthorized software programs can be limited to specific versions or from a specific source. The concept of prohibiting the execution of unauthorized software may also be applied to user actions, system ports and protocols, IP addresses/ranges, websites, and MAC addresses.

Least Functionality | Authorized Software — Allow-by-exception (CM-7(5))

Description for Least Functionality | Authorized Software — Allow-by-exception (CM-7(5))
(a) Identify [Assignment: organization-defined software programs authorized to execute on the system];
(b) Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system; and
(c) Review and update the list of authorized software programs [Assignment: organization-defined frequency].

Discussion for Least Functionality | Authorized Software — Allow-by-exception (CM-7(5))
Authorized software programs can be limited to specific versions or from a specific source. To facilitate a comprehensive authorized software process and increase the strength of protection for attacks that bypass application level authorized software, software programs may be decomposed into and monitored at different levels of detail. These levels include applications, application programming interfaces, application modules, scripts, system processes, system services, kernel functions, registries, drivers, and dynamic link libraries. The concept of permitting the execution of authorized software may also be applied to user actions, system ports and protocols, IP addresses/ranges, websites, and MAC addresses. Organizations consider verifying the integrity of authorized software programs using digital signatures, cryptographic checksums, or hash functions. Verification of authorized software can occur either prior to execution or at system startup. The identification of authorized URLs for websites is addressed in CA-3(5) and SC-7.

Least Functionality | Confined Environments with Limited Privileges (CM-7(6))

Description for Least Functionality | Confined Environments with Limited Privileges (CM-7(6))
Require that the following user-installed software execute in a confined physical or virtual machine environment with limited privileges: [Assignment: organization-defined user-installed software].

Discussion for Least Functionality | Confined Environments with Limited Privileges (CM-7(6))
Organizations identify software that may be of concern regarding its origin or potential for containing malicious code. For this type of software, user installations occur in confined environments of operation to limit or contain damage from malicious code that may be executed.

Least Functionality | Code Execution in Protected Environments (CM-7(7))

Description for Least Functionality | Code Execution in Protected Environments (CM-7(7))
Allow execution of binary or machine-executable code only in confined physical or virtual machine environments and with the explicit approval of [Assignment: organization-defined personnel or roles] when such code is:
(a) Obtained from sources with limited or no warranty; and/or
(b) Without the provision of source code.

Discussion for Least Functionality | Code Execution in Protected Environments (CM-7(7))
Code execution in protected environments applies to all sources of binary or machine-executable code, including commercial software and firmware and open-source software.

Least Functionality | Binary or Machine Executable Code (CM-7(8))

Description for Least Functionality | Binary or Machine Executable Code (CM-7(8))
(a) Prohibit the use of binary or machine-executable code from sources with limited or no warranty or without the provision of source code; and
(b) Allow exceptions only for compelling mission or operational requirements and with the approval of the authorizing official.

Discussion for Least Functionality | Binary or Machine Executable Code (CM-7(8))
Binary or machine executable code applies to all sources of binary or machine-executable code, including commercial software and firmware and open-source software. Organizations assess software products without accompanying source code or from sources with limited or no warranty for potential security impacts. The assessments address the fact that software products without the provision of source code may be difficult to review, repair, or extend. In addition, there may be no owners to make such repairs on behalf of organizations. If open-source software is used, the assessments address the fact that there is no warranty, the open-source software could contain back doors or malware, and there may be no support available.

Least Functionality | Prohibiting The Use of Unauthorized Hardware (CM-7(9))

Description for Least Functionality | Prohibiting The Use of Unauthorized Hardware (CM-7(9))
(a) Identify [Assignment: organization-defined hardware components authorized for system use];
(b) Prohibit the use or connection of unauthorized hardware components;
(c) Review and update the list of authorized hardware components [Assignment: organization-defined frequency].

Discussion for Least Functionality | Prohibiting The Use of Unauthorized Hardware (CM-7(9))
Hardware components provide the foundation for organizational systems and the platform for the execution of authorized software programs. Managing the inventory of hardware components and controlling which hardware components are permitted to be installed or connected to organizational systems is essential in order to provide adequate security.

System Component Inventory (CM-8)

Description for System Component Inventory (CM-8)
a. Develop and document an inventory of system components that:
1. Accurately reflects the system;
2. Includes all components within the system;
3. Does not include duplicate accounting of components or components assigned to any other system;
4. Is at the level of granularity deemed necessary for tracking and reporting; and
5. Includes the following information to achieve system component accountability: [Assignment: organization-defined information deemed necessary to achieve effective system component accountability]; and
b. Review and update the system component inventory [Assignment: organization-defined frequency].

Discussion for System Component Inventory (CM-8)
System components are discrete, identifiable information technology assets that include hardware, software, and firmware. Organizations may choose to implement centralized system component inventories that include components from all organizational systems. In such situations, organizations ensure that the inventories include system-specific information required for component accountability. The information necessary for effective accountability of system components includes the system name, software owners, software version numbers, hardware inventory specifications, software license information, and for networked components, the machine names and network addresses across all implemented protocols (e.g., IPv4, IPv6). Inventory specifications include date of receipt, cost, model, serial number, manufacturer, supplier information, component type, and physical location.
Preventing duplicate accounting of system components addresses the lack of accountability that occurs when component ownership and system association is not known, especially in large or complex connected systems. Effective prevention of duplicate accounting of system components necessitates use of a unique identifier for each component. For software inventory, centrally managed software that is accessed via 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 association 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.

System Component Inventory | Updates During Installation and Removal (CM-8(1))

Description for System Component Inventory | Updates During Installation and Removal (CM-8(1))
Update the inventory of system components as part of component installations, removals, and system updates.

Discussion for System Component Inventory | Updates During Installation and Removal (CM-8(1))
Organizations can improve the accuracy, completeness, and consistency of system component inventories if the inventories are updated as part of component installations or removals or during general system updates. If inventories are not updated at these key times, there is a greater likelihood that the information will not be appropriately captured and documented. System updates include hardware, software, and firmware components.

System Component Inventory | Automated Maintenance (CM-8(2))

Description for System Component Inventory | Automated Maintenance (CM-8(2))
Maintain the currency, completeness, accuracy, and availability of the inventory of system components using [Assignment: organization-defined automated mechanisms].

Discussion for System Component Inventory | Automated Maintenance (CM-8(2))
Organizations maintain system inventories to the extent feasible. For example, virtual machines can be difficult to monitor because such machines are not visible to the network when not in use. In such cases, organizations maintain as up-to-date, complete, and accurate an inventory as is deemed reasonable. Automated maintenance can be achieved by the implementation of CM-2(2) for organizations that combine system component inventory and baseline configuration activities.

System Component Inventory | Automated Unauthorized Component Detection (CM-8(3))

Description for System Component Inventory | Automated Unauthorized Component Detection (CM-8(3))
(a) Detect the presence of unauthorized hardware, software, and firmware components within the system using [Assignment: organization-defined automated mechanisms] [Assignment: organization-defined frequency]; and
(b) Take the following actions when unauthorized components are detected: [Selection (one or more): disable network access by such components; isolate the components; notify [Assignment: organization-defined personnel or roles]].

Discussion for System Component Inventory | Automated Unauthorized Component Detection (CM-8(3))
Automated unauthorized component detection is applied in addition to the monitoring for unauthorized remote connections and mobile devices. Monitoring for unauthorized system components may be accomplished on an ongoing basis or by the periodic scanning of systems for that purpose. Automated mechanisms may also be used to prevent the connection of unauthorized components (see CM-7(9)). Automated mechanisms can be implemented in systems or in separate system components. When acquiring and implementing automated mechanisms, organizations consider whether such mechanisms depend on the ability of the system component to support an agent or supplicant in order to be detected since some types of components do not have or cannot support agents (e.g., IoT devices, sensors). Isolation can be achieved , for example, by placing unauthorized system components in separate domains or subnets or quarantining such

components. This type of component isolation is commonly referred to as sandboxing.

System Component Inventory | Accountability Information (CM-8(4))

Description for System Component Inventory | Accountability Information (CM-8(4))
Include in the system component inventory information, a means for identifying by [Selection (one or more): name; position; role], individuals responsible and accountable for administering those components.

Discussion for System Component Inventory | Accountability Information (CM-8(4))
Identifying individuals who are responsible and accountable for administering system components ensures that the assigned components are properly administered and that organizations can contact those individuals if some action is required (e.g., when the component is determined to be the source of a breach, needs to be recalled or replaced, or needs to be relocated).

Configuration Settings | Conformance Demonstration (CM-6(4))

Description for Configuration Settings | Conformance Demonstration (CM-6(4))
[Withdrawn: Incorporated into CM-4.]

Discussion for Configuration Settings | Conformance Demonstration (CM-6(4))

System Component Inventory | Assessed Configurations and Approved Deviations (CM-8(6))

Description for System Component Inventory | Assessed Configurations and Approved Deviations (CM-8(6))
Include assessed component configurations and any approved deviations to current deployed configurations in the system component inventory.

Discussion for System Component Inventory | Assessed Configurations and Approved Deviations (CM-8(6))
Assessed configurations and approved deviations focus on configuration settings established by organizations for system components, the specific components that have been assessed to determine compliance with the required configuration settings, and any approved deviations from established configuration settings.

System Component Inventory | Centralized Repository (CM-8(7))

Description for System Component Inventory | Centralized Repository (CM-8(7))
Provide a centralized repository for the inventory of system components.

Discussion for System Component Inventory | Centralized Repository (CM-8(7))
Organizations may implement centralized system component inventories that include components from all organizational systems. Centralized repositories of component inventories provide opportunities for efficiencies in accounting for organizational hardware, software, and firmware assets. Such repositories may 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 system-specific information required for proper component accountability.

System Component Inventory | Automated Location Tracking (CM-8(8))

Description for System Component Inventory | Automated Location Tracking (CM-8(8))
Support the tracking of system components by geographic location using [Assignment: organization-defined automated mechanisms].

Discussion for System Component Inventory | Automated Location Tracking (CM-8(8))
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 coordinated with senior agency officials for privacy if there are implications that affect individual privacy.

System Component Inventory | Assignment of Components to Systems (CM-8(9))

Description for System Component Inventory | Assignment of Components to Systems (CM-8(9))
(a) Assign system components to a system; and
(b) Receive an acknowledgement from [Assignment: organization-defined personnel or roles] of this assignment.

Discussion for System Component Inventory | Assignment of Components to Systems (CM-8(9))
System components that are not assigned to a system may be unmanaged, lack the required protection, and become an organizational vulnerability.

Configuration Management Plan (CM-9)

Description for Configuration Management Plan (CM-9)
Develop, document, and implement a configuration management plan for the system that:
a. Addresses roles, responsibilities, and configuration management processes and procedures;
b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;
c. Defines the configuration items for the system and places the configuration items under configuration management;
d. Is reviewed and approved by [Assignment: organization-defined personnel or roles]; and
e. Protects the configuration management plan from unauthorized disclosure and modification.

Discussion for Configuration Management Plan (CM-9)
Configuration management activities occur throughout the system development life cycle. As such, there are developmental configuration management activities (e.g., the control of code and software libraries) and operational configuration management activities (e.g., control of installed components and how the components are configured). Configuration management plans satisfy the requirements in configuration management policies while being tailored to individual systems. Configuration management plans define processes and procedures for how configuration management is used to support system development life cycle activities.
Configuration management plans are generated during the development and acquisition stage of the system development life cycle. The plans describe how to advance changes through change management processes; update configuration settings and baselines; maintain component inventories; control development, test, and operational environments; and develop, release, and update key documents.
Organizations can employ templates to help ensure the consistent and timely development and implementation of configuration management plans. Templates can represent a configuration management plan for the organization with subsets of the plan implemented on a system by system basis. Configuration management approval processes include the designation of key stakeholders responsible for reviewing and approving proposed changes to systems, and personnel who conduct security and privacy impact analyses prior to the implementation of changes to the systems. Configuration items are the system components, such as the hardware, software, firmware, and documentation to be configuration-managed. As systems continue through the system development life cycle, new

configuration items may be identified, and some existing configuration items may no longer need to be under configuration control.

Configuration Management Plan | Assignment of Responsibility (CM-9(1))

Description for Configuration Management Plan | Assignment of Responsibility (CM-9(1))
Assign responsibility for developing the configuration management process to organizational personnel that are not directly involved in system development.

Discussion for Configuration Management Plan | Assignment of Responsibility (CM-9(1))
In the absence of dedicated configuration management teams assigned within organizations, system developers may be tasked with developing configuration management processes using personnel who are not directly involved in system development or system integration. This separation of duties ensures that organizations establish and maintain a sufficient degree of independence between the system development and integration processes and configuration management processes to facilitate quality control and more effective oversight.

Software Usage Restrictions (CM-10)

Description for Software Usage Restrictions (CM-10)
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 the unauthorized distribution, display, performance, or reproduction of copyrighted work.

Discussion for Software Usage Restrictions (CM-10)
Software license tracking can be accomplished by manual or automated methods, depending on organizational needs. Examples of contract agreements include software license agreements and non-disclosure agreements.

Software Usage Restrictions | Open-source Software (CM-10(1))

Description for Software Usage Restrictions | Open-source Software (CM-10(1))
Establish the following restrictions on the use of open-source software: [Assignment: organization-defined restrictions].

Discussion for Software Usage Restrictions | Open-source Software (CM-10(1))
Open-source software refers to software that is available in source code form. Certain software rights normally reserved for copyright holders are routinely 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. In some cases, there is an online community associated with the software that inspects, tests, updates, and reports on issues found in software on an ongoing basis. However, remediating vulnerabilities in open-source software may be problematic. There may also be licensing issues associated with open-source software, including the constraints on derivative use of such software. Open-source software that is available only in binary form may increase the level of risk in using such software.

User-installed Software (CM-11)

Description for User-installed Software (CM-11)
a. Establish [Assignment: organization-defined policies] governing the installation of software by users;
b. Enforce software installation policies through the following methods: [Assignment: organization-defined methods]; and
c. Monitor policy compliance [Assignment: organization-defined frequency].

Discussion for User-installed Software (CM-11)
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 organization-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.

System Component Inventory | No Duplicate Accounting of Components (CM-8(5))

Description for System Component Inventory | No Duplicate Accounting of Components (CM-8(5))
[Withdrawn: Incorporated into CM-8.]

Discussion for System Component Inventory | No Duplicate Accounting of Components (CM-8(5))

User-installed Software | Software Installation with Privileged Status (CM-11(2))

Description for User-installed Software | Software Installation with Privileged Status (CM-11(2))
Allow user installation of software only with explicit privileged status.

Discussion for User-installed Software | Software Installation with Privileged Status (CM-11(2))
Privileged status can be obtained, for example, by serving in the role of system administrator.

User-installed Software | Automated Enforcement and Monitoring (CM-11(3))

Description for User-installed Software | Automated Enforcement and Monitoring (CM-11(3))
Enforce and monitor compliance with software installation policies using [Assignment: organization-defined automated mechanisms].

Discussion for User-installed Software | Automated Enforcement and Monitoring (CM-11(3))
Organizations enforce and monitor compliance with software installation policies using automated mechanisms to more quickly detect and respond to unauthorized software installation which can be an indicator of an internal or external hostile attack.

Information Location (CM-12)

Description for Information Location (CM-12)
a. Identify and document the location of [Assignment: organization-defined information] and the specific system components on which the information is processed and stored;
b. Identify and document the users who have access to the system and system components where the information is processed and stored; and
c. Document changes to the location (i.e., system or system components) where the information is processed and stored.

Discussion for Information Location (CM-12)
Information location addresses the need to understand where information is being processed and stored. Information location includes identifying where specific information types and information reside in system components 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 information and the system component where the information resides (see FIPS 199). The location of the information and system components is also a factor in the architecture and design of the system (see SA-4, SA-8, SA-17).

Information Location | Automated Tools to Support Information Location (CM-12(1))

Description for Information Location | Automated Tools to Support Information Location (CM-12(1))
Use automated tools to identify [Assignment: organization-defined information by information type] on [Assignment: organization-defined system components] to ensure controls are in place to protect organizational information and individual privacy.

Discussion for Information Location | Automated Tools to Support Information Location (CM-12(1))
The use of automated tools helps to increase the effectiveness and efficiency of the information location capability implemented within the system. Automation also helps organizations manage the data produced during information location activities and share such information across the organization. The output of automated information location tools can be used to guide and inform system architecture and design decisions.

Data Action Mapping (CM-13)

Description for Data Action Mapping (CM-13)
Develop and document a map of system data actions.

Discussion for Data Action Mapping (CM-13)
Data actions are system operations that process personally identifiable information. The processing of such information encompasses the full information life cycle, which includes collection, generation, transformation, use, disclosure, retention, and disposal. A map of system data actions includes discrete data actions, elements of personally identifiable information being processed in the data actions, system components involved in the data actions, and the owners or operators of the system 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 in another part of the system), and by whom (e.g., individuals may have different privacy perceptions 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 created by the system. Data maps can be illustrated in different

ways, and the level of detail may vary based on the mission and business needs of the organization. The data map may be an overlay 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.

Signed Components (CM-14)

Description for Signed Components (CM-14)
Prevent the installation of [Assignment: organization-defined software and firmware components] without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

Discussion for Signed Components (CM-14)
Software and firmware components prevented from installation unless signed with recognized and approved certificates include software and firmware version updates, patches, service packs, device drivers, and basic input/output system updates. Organizations can identify applicable software and firmware components by type, by specific items, or a combination of both. Digital signatures and organizational verification of such signatures is a method of code authentication.

Policy and Procedures (CP-1)

Description for Policy and Procedures (CP-1)
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] contingency planning policy that:
(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the contingency planning policy and the associated contingency planning controls;
b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the contingency planning policy and procedures; and
c. Review and update the current contingency planning:
1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

Discussion for Policy and Procedures (CP-1)
Contingency planning policy and procedures address the controls in the CP family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of contingency planning policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, 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. Events that may precipitate an update to contingency planning policy and procedures include assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Contingency Plan (CP-2)

Description for Contingency Plan (CP-2)
a. Develop a contingency plan for the system that:
1. Identifies essential mission and business functions and associated contingency requirements;
2. Provides recovery objectives, restoration priorities, and metrics;
3. Addresses contingency roles, responsibilities, assigned individuals with contact information;
4. Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure;
5. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented;
6. Addresses the sharing of contingency information; and
7. Is reviewed and approved by [Assignment: organization-defined personnel or roles];
b. Distribute copies of the contingency plan to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements];
c. Coordinate contingency planning activities with incident handling activities;
d. Review the contingency plan for the system [Assignment: organization-defined frequency];
e. Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;
f. Communicate contingency plan changes to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements];
g. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training; and
h. Protect the contingency plan from unauthorized disclosure and modification.

Discussion for Contingency Plan (CP-2)
Contingency planning for systems is part of an overall program for achieving continuity of operations for organizational mission and business functions. Contingency planning addresses system restoration and implementation of alternative mission or business processes when systems are compromised or breached. Contingency planning is considered throughout the system development life cycle and is a fundamental part of the system design. Systems can be designed for redundancy, to provide backup capabilities, and for resilience. Contingency plans reflect the degree of restoration required for organizational systems since not all systems need to fully recover to achieve the level of continuity of operations desired. System recovery objectives reflect applicable laws, executive orders, directives, regulations, policies, standards, guidelines,

organizational risk tolerance, and system impact level.
Actions addressed in contingency plans include orderly system degradation, system shutdown, fallback to a manual mode, alternate information flows, and operating in modes reserved for when systems are under attack. By coordinating contingency planning with incident handling activities, organizations ensure that the necessary planning activities are in place and activated in the event of an incident. Organizations consider whether continuity of operations during an incident conflicts with the capability to automatically disable the system, as specified in IR-4(5). Incident response planning is part of contingency planning for organizations and is addressed in the IR (Incident Response) family.

Contingency Plan | Coordinate with Related Plans (CP-2(1))

Description for Contingency Plan | Coordinate with Related Plans (CP-2(1))
Coordinate contingency plan development with organizational elements responsible for related plans.

Discussion for Contingency Plan | Coordinate with Related Plans (CP-2(1))
Plans that are related to contingency plans include Business Continuity Plans, Disaster Recovery Plans, Critical Infrastructure Plans, Continuity of Operations Plans, Crisis Communications Plans, Insider Threat Implementation Plans, Data Breach Response Plans, Cyber Incident Response Plans, Breach Response Plans, and Occupant Emergency Plans.

Contingency Plan | Capacity Planning (CP-2(2))

Description for Contingency Plan | Capacity Planning (CP-2(2))
Conduct capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.

Discussion for Contingency Plan | Capacity Planning (CP-2(2))
Capacity planning is needed because different threats can result in a reduction of the available processing, telecommunications, and support services intended to support essential mission 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 in a degraded state. Such

determinations are based on an organizational assessment of risk, system categorization (impact level), and organizational risk tolerance.

Contingency Plan | Resume Mission and Business Functions (CP-2(3))

Description for Contingency Plan | Resume Mission and Business Functions (CP-2(3))
Plan for the resumption of [Selection: all; essential] mission and business functions within [Assignment: organization-defined time period] of contingency plan activation.

Discussion for Contingency Plan | Resume Mission and Business Functions (CP-2(3))
Organizations may choose to conduct contingency planning activities to resume mission and business functions as part of business continuity planning or as part of business impact analyses. Organizations prioritize the resumption of mission and business functions. The time period for resuming mission and business functions may be dependent on the severity and extent of the disruptions to the system and its supporting infrastructure.

System Recovery and Reconstitution | Contingency Plan Testing (CP-10(1))

Description for System Recovery and Reconstitution | Contingency Plan Testing (CP-10(1))
[Withdrawn: Incorporated into CP-4.]

Discussion for System Recovery and Reconstitution | Contingency Plan Testing (CP-10(1))

Contingency Plan | Continue Mission and Business Functions (CP-2(5))

Description for Contingency Plan | Continue Mission and Business Functions (CP-2(5))
Plan for the continuance of [Selection: all; essential] mission and business functions with minimal or no loss of operational continuity and sustains that continuity until full system restoration at primary processing and/or storage sites.

Discussion for Contingency Plan | Continue Mission and Business Functions (CP-2(5))
Organizations may choose to conduct the contingency planning activities to continue mission and business functions as part of business continuity planning or business impact analyses. Primary processing and/or storage sites defined by organizations as part of contingency planning may change depending on the circumstances associated with the contingency.

Contingency Plan | Alternate Processing and Storage Sites (CP-2(6))

Description for Contingency Plan | Alternate Processing and Storage Sites (CP-2(6))
Plan for the transfer of [Selection: all; essential] mission and business functions to alternate processing and/or storage sites with minimal or no loss of operational continuity and sustain that continuity through system restoration to primary processing and/or storage sites.

Discussion for Contingency Plan | Alternate Processing and Storage Sites (CP-2(6))
Organizations may choose to conduct contingency planning activities for alternate processing and storage sites as part of business continuity planning or business impact analyses. Primary processing and/or storage sites defined by organizations as part of contingency planning may change depending on the circumstances associated with the contingency.

Contingency Plan | Coordinate with External Service Providers (CP-2(7))

Description for Contingency Plan | Coordinate with External Service Providers (CP-2(7))
Coordinate the contingency plan with the contingency plans of external service providers to ensure that contingency requirements can be satisfied.

Discussion for Contingency Plan | Coordinate with External Service Providers (CP-2(7))
When the capability of an organization to carry out its mission and business functions is dependent on external service providers, developing a comprehensive and timely contingency plan may become more challenging. When mission and business functions are dependent on external service providers, organizations coordinate contingency planning activities with the external entities to ensure that the individual plans reflect the overall contingency needs of the organization.

Contingency Plan | Identify Critical Assets (CP-2(8))

Description for Contingency Plan | Identify Critical Assets (CP-2(8))
Identify critical system assets supporting [Selection: all; essential] mission and business functions.

Discussion for Contingency Plan | Identify Critical Assets (CP-2(8))
Organizations may choose to identify critical assets as part of criticality analysis, business continuity planning, or business impact analyses. Organizations identify critical system assets so that additional controls can be employed (beyond the controls routinely implemented) to help ensure that organizational mission and business functions can continue to be conducted during contingency operations. The identification of critical information assets also facilitates the prioritization of organizational resources. Critical system assets include technical and operational aspects. Technical aspects include system components, information technology services, information technology products, and mechanisms. Operational aspects include procedures (i.e., manually executed operations) and personnel (i.e., individuals operating technical controls and/or executing manual procedures). Organizational program protection plans can assist in identifying critical assets. If critical assets are resident within or supported by external service providers, organizations consider implementing CP-2(7) as a control enhancement.

Contingency Training (CP-3)

Description for Contingency Training (CP-3)
a. Provide contingency training to system users consistent with assigned roles and responsibilities:
1. Within [Assignment: organization-defined time period] of assuming a contingency role or responsibility;
2. When required by system changes; and
3. [Assignment: organization-defined frequency] thereafter; and
b. Review and update contingency training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

Discussion for Contingency Training (CP-3)
Contingency training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail is included in such training. For example, some individuals may only need to know when and where to report for duty during contingency operations and if normal duties are affected; system administrators may require additional training on how to establish systems at alternate processing and storage sites; and organizational officials may receive more specific training on how to conduct mission-essential functions in designated off-site locations and how to establish communications with other governmental entities for purposes of coordination on contingency-related activities. Training for contingency roles or responsibilities reflects the specific continuity requirements in the contingency plan. Events that may precipitate an update to contingency training content include, but are not limited to, contingency plan testing or an actual contingency (lessons learned), assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. At the discretion of the organization, participation in a contingency plan test or exercise, including lessons learned sessions subsequent to the test or exercise, may satisfy contingency plan training requirements.

Contingency Training | Simulated Events (CP-3(1))

Description for Contingency Training | Simulated Events (CP-3(1))
Incorporate simulated events into contingency training to facilitate effective response by personnel in crisis situations.

Discussion for Contingency Training | Simulated Events (CP-3(1))
The use of simulated events creates an environment for personnel to experience actual threat events, including cyber-attacks that disable websites, ransomware attacks that encrypt organizational data on servers, hurricanes that damage or destroy organizational facilities, or hardware or software failures.

Contingency Training | Mechanisms Used in Training Environments (CP-3(2))

Description for Contingency Training | Mechanisms Used in Training Environments (CP-3(2))
Employ mechanisms used in operations to provide a more thorough and realistic contingency training environment.

Discussion for Contingency Training | Mechanisms Used in Training Environments (CP-3(2))
Operational mechanisms refer to processes that have been established to accomplish an organizational goal or a system that supports a particular organizational mission or business objective. Actual mission and business processes, systems, and/or facilities may be used to generate simulated events and enhance the realism of simulated events during contingency training.

Contingency Plan Testing (CP-4)

Description for Contingency Plan Testing (CP-4)
a. Test the contingency plan for the system [Assignment: organization-defined frequency] using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: [Assignment: organization-defined tests].
b. Review the contingency plan test results; and
c. Initiate corrective actions, if needed.

Discussion for Contingency Plan Testing (CP-4)
Methods for testing contingency plans to determine the effectiveness of the plans and identify potential weaknesses include checklists, walk-through and tabletop exercises, simulations (parallel or full interrupt), and comprehensive exercises. Organizations conduct testing based on the requirements in contingency plans and include a determination of the effects on organizational operations, assets, and individuals due to contingency operations. Organizations have flexibility and discretion in the breadth, depth, and timelines of corrective actions.

Contingency Plan Testing | Coordinate with Related Plans (CP-4(1))

Description for Contingency Plan Testing | Coordinate with Related Plans (CP-4(1))
Coordinate contingency plan testing with organizational elements responsible for related plans.

Discussion for Contingency Plan Testing | Coordinate with Related Plans (CP-4(1))
Plans related to contingency planning for organizational systems include Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, and Occupant Emergency Plans. Coordination of contingency plan testing does not require organizations to create organizational elements to handle related plans or to align such elements with specific plans. However, it does require that if such organizational elements are responsible for related plans, organizations coordinate with those elements.

Contingency Plan Testing | Alternate Processing Site (CP-4(2))

Description for Contingency Plan Testing | Alternate Processing Site (CP-4(2))
Test the contingency plan at the alternate processing site:
(a) To familiarize contingency personnel with the facility and available resources; and
(b) To evaluate the capabilities of the alternate processing site to support contingency operations.

Discussion for Contingency Plan Testing | Alternate Processing Site (CP-4(2))
Conditions at the alternate processing site may be significantly different than the conditions at the primary site. Having the opportunity to visit the alternate site and experience the actual capabilities available at the site can provide valuable information on potential vulnerabilities that could affect essential organizational mission and business functions. The on-site visit can also provide an opportunity to refine the contingency plan to address the vulnerabilities discovered during testing.

Contingency Plan Testing | Automated Testing (CP-4(3))

Description for Contingency Plan Testing | Automated Testing (CP-4(3))
Test the contingency plan using [Assignment: organization-defined automated mechanisms].

Discussion for Contingency Plan Testing | Automated Testing (CP-4(3))
Automated mechanisms facilitate thorough and effective testing of contingency plans by providing more complete coverage of contingency issues, selecting more realistic test scenarios and environments, and effectively stressing the system and supported mission and business functions.

Contingency Plan Testing | Full Recovery and Reconstitution (CP-4(4))

Description for Contingency Plan Testing | Full Recovery and Reconstitution (CP-4(4))
Include a full recovery and reconstitution of the system to a known state as part of contingency plan testing.

Discussion for Contingency Plan Testing | Full Recovery and Reconstitution (CP-4(4))
Recovery is executing contingency plan activities to restore organizational mission and business functions. Reconstitution takes place following recovery and includes activities for returning systems to fully operational states. Organizations establish a known state for systems that includes system state information for hardware, software programs, and data. Preserving system state information facilitates system restart and return to the operational mode of organizations with less disruption of mission and business processes.

Contingency Plan Testing | Self-challenge (CP-4(5))

Description for Contingency Plan Testing | Self-challenge (CP-4(5))
Employ [Assignment: organization-defined mechanisms] to [Assignment: organization-defined system or system component] to disrupt and adversely affect the system or system component.

Discussion for Contingency Plan Testing | Self-challenge (CP-4(5))
Often, the best method of assessing system resilience is to disrupt the system in some manner. The mechanisms used by the organization could disrupt system functions or system services in many ways, including terminating or disabling critical system components, changing the configuration of system components, degrading critical functionality (e.g., restricting network bandwidth), or altering privileges. Automated, on-going, and simulated cyber-attacks and service disruptions can reveal unexpected functional dependencies and help the organization determine its ability to ensure resilience in the face of an actual cyber-attack.

System Recovery and Reconstitution | Compensating Security Controls (CP-10(3))

Description for System Recovery and Reconstitution | Compensating Security Controls (CP-10(3))
[Withdrawn: Addressed through tailoring.]

Discussion for System Recovery and Reconstitution | Compensating Security Controls (CP-10(3))

Alternate Storage Site (CP-6)

Description for Alternate Storage Site (CP-6)
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.

Discussion for Alternate Storage Site (CP-6)
Alternate storage sites are geographically distinct from primary storage sites and maintain duplicate copies of information and data if the primary storage site is not available. Similarly, alternate processing sites provide processing capability if the primary processing site is not available. Geographically distributed architectures that support contingency requirements may be considered alternate storage sites. Items 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 mission and business functions despite compromise, failure, or disruption in organizational systems.

Alternate Storage Site | Separation from Primary Site (CP-6(1))

Description for Alternate Storage Site | Separation from Primary Site (CP-6(1))
Identify an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats.

Discussion for Alternate Storage Site | Separation from Primary Site (CP-6(1))
Threats that affect alternate storage sites are defined in organizational risk assessments and include natural disasters, structural failures, hostile attacks, and errors of 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.

Alternate Storage Site | Recovery Time and Recovery Point Objectives (CP-6(2))

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

Discussion for Alternate Storage Site | Recovery Time and Recovery Point Objectives (CP-6(2))
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 that ensure accessibility and correct execution.

Alternate Storage Site | Accessibility (CP-6(3))

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

Discussion for Alternate Storage Site | Accessibility (CP-6(3))
Area-wide disruptions refer to those types of disruptions that are broad 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 at originally designated alternate sites or planning for physical access to retrieve backup information if electronic accessibility to the alternate site is disrupted.

Alternate Processing Site (CP-7)

Description for Alternate Processing Site (CP-7)
a. Establish an alternate processing site, including necessary agreements to permit the transfer and resumption of [Assignment: organization-defined system operations] for essential mission and business functions within [Assignment: organization-defined 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 to 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.

Discussion for Alternate Processing Site (CP-7)
Alternate processing sites 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 failover to a cloud-based service provider or other internally or externally provided processing service. Geographically distributed architectures that support contingency requirements may also be considered alternate processing sites. Controls that are covered by alternate processing site agreements include the environmental conditions at alternate sites, access rules, physical and environmental protection requirements, and the coordination for the transfer and assignment of personnel. Requirements are allocated to alternate processing sites that reflect the requirements in contingency plans to maintain essential mission and business functions despite disruption, compromise, or failure in organizational systems.

Alternate Processing Site | Separation from Primary Site (CP-7(1))

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

Discussion for Alternate Processing Site | Separation from Primary Site (CP-7(1))
Threats that affect alternate processing sites are defined in organizational assessments of risk and include natural disasters, structural failures, hostile attacks, and errors of 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.

Alternate Processing Site | Accessibility (CP-7(2))

Description for Alternate Processing Site | Accessibility (CP-7(2))
Identify potential accessibility problems to alternate processing sites in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

Discussion for Alternate Processing Site | Accessibility (CP-7(2))
Area-wide disruptions refer to those types of disruptions that are broad in geographic scope with such determinations made by organizations based on organizational assessments of risk.

Alternate Processing Site | Priority of Service (CP-7(3))

Description for Alternate Processing Site | Priority of Service (CP-7(3))
Develop alternate processing site agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives).

Discussion for Alternate Processing Site | Priority of Service (CP-7(3))
Priority of service agreements refer to negotiated agreements with service providers that ensure that organizations receive priority treatment consistent with their availability requirements and the availability of information resources for logical alternate processing and/or at the physical alternate processing site. Organizations establish recovery time objectives as part of contingency planning.

Alternate Processing Site | Preparation for Use (CP-7(4))

Description for Alternate Processing Site | Preparation for Use (CP-7(4))
Prepare the alternate processing site so that the site can serve as the operational site supporting essential mission and business functions.

Discussion for Alternate Processing Site | Preparation for Use (CP-7(4))
Site preparation includes establishing configuration settings for systems at 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.

System Recovery and Reconstitution | Failover Capability (CP-10(5))

Description for System Recovery and Reconstitution | Failover Capability (CP-10(5))
[Withdrawn: Incorporated into SI-13.]

Discussion for System Recovery and Reconstitution | Failover Capability (CP-10(5))

Alternate Processing Site | Inability to Return to Primary Site (CP-7(6))

Description for Alternate Processing Site | Inability to Return to Primary Site (CP-7(6))
Plan and prepare for circumstances that preclude returning to the primary processing site.

Discussion for Alternate Processing Site | Inability to Return to Primary Site (CP-7(6))
There may be situations that preclude an organization from returning to the primary processing site such as if a natural disaster (e.g., flood or a hurricane) damaged or destroyed a facility and it was determined that rebuilding in the same location was not prudent.

Telecommunications Services (CP-8)

Description for Telecommunications Services (CP-8)
Establish alternate telecommunications services, including necessary agreements to permit the resumption of [Assignment: organization-defined system operations] for essential mission and business functions within [Assignment: organization-defined time period] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

Discussion for Telecommunications Services (CP-8)
Telecommunications services (for data and voice) for primary and alternate processing and storage sites are in scope for CP-8. Alternate telecommunications services reflect the continuity requirements in contingency plans to maintain essential mission 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, network-based approaches to telecommunications, or the use of satellites. Organizations consider factors such as availability, quality of service, and access when entering into alternate telecommunications agreements.

Telecommunications Services | Priority of Service Provisions (CP-8(1))

Description for Telecommunications Services | Priority of Service Provisions (CP-8(1))
(a) Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives); and
(b) Request Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness if the primary and/or alternate telecommunications services are provided by a common carrier.

Discussion for Telecommunications Services | Priority of Service Provisions (CP-8(1))
Organizations consider the potential mission or business impact in situations where telecommunications service providers are servicing other organizations with similar priority of service provisions. Telecommunications Service Priority (TSP) is a Federal Communications Commission (FCC) program that directs telecommunications service providers (e.g., wireline and wireless phone companies) to give preferential treatment to users enrolled in the program when they need to add new lines or have their lines restored following 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 attack taking place. Federal sponsorship is required to enroll in the TSP program.

Telecommunications Services | Single Points of Failure (CP-8(2))

Description for Telecommunications Services | Single Points of Failure (CP-8(2))
Obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

Discussion for Telecommunications Services | Single Points of Failure (CP-8(2))
In certain circumstances, telecommunications service providers or services may share the same physical lines, which increases the vulnerability of a single failure point. It is important to have provider transparency for the actual physical transmission capability for telecommunication services.

Telecommunications Services | Separation of Primary and Alternate Providers (CP-8(3))

Description for Telecommunications Services | Separation of Primary and Alternate Providers (CP-8(3))
Obtain alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.

Discussion for Telecommunications Services | Separation of Primary and Alternate Providers (CP-8(3))
Threats that affect telecommunications services are defined in organizational assessments of risk and include natural disasters, structural failures, cyber or physical attacks, and errors of omission or commission. Organizations can reduce common susceptibilities by minimizing shared infrastructure among telecommunications service providers and achieving sufficient geographic separation between services. Organizations may consider using a single service provider in situations where the service provider can provide alternate telecommunications services that meet the separation needs addressed in the risk assessment.

Telecommunications Services | Provider Contingency Plan (CP-8(4))

Description for Telecommunications Services | Provider Contingency Plan (CP-8(4))
(a) Require primary and alternate telecommunications service providers to have contingency plans;
(b) Review provider contingency plans to ensure that the plans meet organizational contingency requirements; and
(c) Obtain evidence of contingency testing and training by providers [Assignment: organization-defined frequency].

Discussion for Telecommunications Services | Provider Contingency Plan (CP-8(4))
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 and state and local governments. Organizations may use these types of activities to satisfy evidentiary requirements related to service provider contingency plan reviews, testing, and training.

Telecommunications Services | Alternate Telecommunication Service Testing (CP-8(5))

Description for Telecommunications Services | Alternate Telecommunication Service Testing (CP-8(5))
Test alternate telecommunication services [Assignment: organization-defined frequency].

Discussion for Telecommunications Services | Alternate Telecommunication Service Testing (CP-8(5))
Alternate telecommunications services testing is arranged through contractual agreements with service providers. The testing may occur in parallel with normal operations to ensure that there is no degradation in organizational missions or functions.

System Backup (CP-9)

Description for System Backup (CP-9)
a. Conduct backups of user-level information contained in [Assignment: organization-defined system components] [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives];
b. Conduct backups of system-level information contained in the system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives];
c. Conduct backups of system documentation, including security- and privacy-related documentation [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; and
d. Protect the confidentiality, integrity, and availability of backup information.

Discussion for System Backup (CP-9)
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 system backup information while in transit is addressed by MP-5 and SC-8. System backups reflect the requirements in contingency plans as well as other organizational requirements for backing up 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.

System Backup | Testing for Reliability and Integrity (CP-9(1))

Description for System Backup | Testing for Reliability and Integrity (CP-9(1))
Test backup information [Assignment: organization-defined frequency] to verify media reliability and information integrity.

Discussion for System Backup | Testing for Reliability and Integrity (CP-9(1))
Organizations need assurance that backup information can be reliably retrieved. Reliability pertains to the systems and system components where the backup information is stored, the operations used to retrieve the information, and the integrity of the information being retrieved. Independent and specialized tests can be used for each of the aspects of reliability. For example, decrypting and transporting (or transmitting) 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.

System Backup | Test Restoration Using Sampling (CP-9(2))

Description for System Backup | Test Restoration Using Sampling (CP-9(2))
Use a sample of backup information in the restoration of selected system functions as part of contingency plan testing.

Discussion for System Backup | Test Restoration Using Sampling (CP-9(2))
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 retrieved to determine whether the functions are operating as intended. Organizations can determine the sample size for the functions and backup information based on the level of assurance needed.

System Backup | Separate Storage for Critical Information (CP-9(3))

Description for System Backup | Separate Storage for Critical Information (CP-9(3))
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.

Discussion for System Backup | Separate Storage for Critical Information (CP-9(3))
Separate storage for critical information applies to all critical information regardless of the type of backup storage media. Critical system software includes operating systems, 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 at alternative storage sites (e.g., data centers). The General Services Administration (GSA) establishes standards and specifications for security and fire rated containers.

Contingency Plan | Resume All Mission and Business Functions (CP-2(4))

Description for Contingency Plan | Resume All Mission and Business Functions (CP-2(4))
[Withdrawn: Incorporated into CP-2(3).]

Discussion for Contingency Plan | Resume All Mission and Business Functions (CP-2(4))

System Backup | Transfer to Alternate Storage Site (CP-9(5))

Description for System Backup | Transfer to Alternate Storage Site (CP-9(5))
Transfer system backup information to the alternate storage site [Assignment: organization-defined time period and transfer rate consistent with the recovery time and recovery point objectives].

Discussion for System Backup | Transfer to Alternate Storage Site (CP-9(5))
System backup information can be transferred to alternate storage sites either electronically or by the physical shipment of storage media.

System Backup | Redundant Secondary System (CP-9(6))

Description for System Backup | Redundant Secondary System (CP-9(6))
Conduct system backup by maintaining a redundant secondary system that is not collocated with the primary system and that can be activated without loss of information or disruption to operations.

Discussion for System Backup | Redundant Secondary System (CP-9(6))
The effect of system backup can be achieved by maintaining a redundant secondary system that mirrors the primary system, including the replication of information. If this type of redundancy is in place and there is sufficient geographic separation between the two systems, the secondary system can also serve as the alternate processing site.

System Backup | Dual Authorization for Deletion or Destruction (CP-9(7))

Description for System Backup | Dual Authorization for Deletion or Destruction (CP-9(7))
Enforce dual authorization for the deletion or destruction of [Assignment: organization-defined backup information].

Discussion for System Backup | Dual Authorization for Deletion or Destruction (CP-9(7))
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 destruction 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.

System Backup | Cryptographic Protection (CP-9(8))

Description for System Backup | Cryptographic Protection (CP-9(8))
Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of [Assignment: organization-defined backup information].

Discussion for System Backup | Cryptographic Protection (CP-9(8))
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. Cryptographic protection applies to system backup information in storage at both primary and alternate locations. Organizations that implement cryptographic mechanisms to protect information at rest also consider cryptographic key management solutions.

System Recovery and Reconstitution (CP-10)

Description for System Recovery and Reconstitution (CP-10)
Provide for the recovery and reconstitution of the system to a known state within [Assignment: organization-defined time period consistent with recovery time and recovery point objectives] after a disruption, compromise, or failure.

Discussion for System Recovery and Reconstitution (CP-10)
Recovery is executing contingency plan activities to restore organizational mission and business functions. Reconstitution takes place following recovery and includes activities for returning 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, reestablishment of continuous monitoring activities, system reauthorization (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.

Contingency Plan Update (CP-5)

Description for Contingency Plan Update (CP-5)
[Withdrawn: Incorporated into CP-2.]

Discussion for Contingency Plan Update (CP-5)

System Recovery and Reconstitution | Transaction Recovery (CP-10(2))

Description for System Recovery and Reconstitution | Transaction Recovery (CP-10(2))
Implement transaction recovery for systems that are transaction-based.

Discussion for System Recovery and Reconstitution | Transaction Recovery (CP-10(2))
Transaction-based systems include database management systems and transaction processing systems. Mechanisms supporting transaction recovery include transaction rollback and transaction journaling.

Alternate Processing Site | Equivalent Information Security Safeguards (CP-7(5))

Description for Alternate Processing Site | Equivalent Information Security Safeguards (CP-7(5))
Withdrawn: Incorporated into CP-7.]

Discussion for Alternate Processing Site | Equivalent Information Security Safeguards (CP-7(5))

System Recovery and Reconstitution | Restore Within Time Period (CP-10(4))

Description for System Recovery and Reconstitution | Restore Within Time Period (CP-10(4))
Provide the capability to restore system components within [Assignment: organization-defined restoration time periods] from configuration-controlled and integrity-protected information representing a known, operational state for the components.

Discussion for System Recovery and Reconstitution | Restore Within Time Period (CP-10(4))
Restoration of system components includes reimaging, which restores the components to known, operational states.

System Backup | Protection from Unauthorized Modification (CP-9(4))

Description for System Backup | Protection from Unauthorized Modification (CP-9(4))
[Withdrawn: Incorporated into CP-9.]

Discussion for System Backup | Protection from Unauthorized Modification (CP-9(4))

System Recovery and Reconstitution | Component Protection (CP-10(6))

Description for System Recovery and Reconstitution | Component Protection (CP-10(6))
Protect system components used for recovery and reconstitution.

Discussion for System Recovery and Reconstitution | Component Protection (CP-10(6))
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, compilers, and other system software.

Alternate Communications Protocols (CP-11)

Description for Alternate Communications Protocols (CP-11)
Provide the capability to employ [Assignment: organization-defined alternative communications protocols] in support of maintaining continuity of operations.

Discussion for Alternate Communications Protocols (CP-11)
Contingency plans and the contingency training or testing associated with those plans incorporate an alternate communications protocol capability as part of establishing resilience in organizational systems. Switching communications protocols may affect software applications and operational aspects of systems. Organizations assess the potential side effects of introducing alternate communications protocols prior to implementation.

Safe Mode (CP-12)

Description for Safe Mode (CP-12)
When [Assignment: organization-defined conditions] are detected, enter a safe mode of operation with [Assignment: organization-defined restrictions of safe mode of operation].

Discussion for Safe Mode (CP-12)
For systems that support critical mission and business functions—including military operations, civilian space operations, nuclear power plant operations, and air traffic control operations (especially real-time operational environments)—organizations can identify certain conditions under which those systems revert to a predefined safe mode of operation. The safe mode of operation, which can be activated either automatically or manually, restricts the operations that systems can execute when those conditions are encountered. Restriction includes allowing only selected functions to execute that can be carried out under limited power or with reduced communications bandwidth.

Alternative Security Mechanisms (CP-13)

Description for Alternative Security Mechanisms (CP-13)
Employ [Assignment: organization-defined alternative or supplemental security mechanisms] for satisfying [Assignment: organization-defined security functions] when the primary means of implementing the security function is unavailable or compromised.

Discussion for Alternative Security Mechanisms (CP-13)
Use of alternative security mechanisms supports system resiliency, contingency planning, and continuity of operations. To ensure mission and business continuity, organizations can implement alternative or supplemental security mechanisms. The mechanisms may be less effective than the primary mechanisms. However, having the capability to readily employ alternative or supplemental mechanisms enhances mission and business continuity that might otherwise be adversely impacted if operations had to be curtailed until the primary means of implementing the functions was restored. Given the cost and level of effort required to provide such alternative capabilities, the alternative or supplemental mechanisms are only applied to critical security capabilities provided by systems, system components, or system services. For example, an organization may issue one-time pads to senior executives, officials, and system administrators if multi-factor tokens—the standard means for achieving secure authentication— are compromised.

Policy and Procedures (IA-1)

Description for Policy and Procedures (IA-1)
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] identification and authentication policy that:
(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls;
b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the identification and authentication policy and procedures; and
c. Review and update the current identification and authentication:
1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

Discussion for Policy and Procedures (IA-1)
Identification and authentication policy and procedures address the controls in the IA family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of identification and authentication policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, 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. Events that may precipitate an update to identification and authentication policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Identification and Authentication (organizational Users) (IA-2)

Description for Identification and Authentication (organizational Users) (IA-2)
Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

Discussion for Identification and Authentication (organizational Users) (IA-2)
Organizations can satisfy the identification and authentication requirements by complying with the requirements in HSPD 12. Organizational users include employees or individuals who organizations consider to have an equivalent status to employees (e.g., contractors and guest researchers). Unique identification and authentication of users applies to all accesses other than those that are explicitly identified in AC-14 and that occur through the authorized use of group authenticators without individual authentication. Since processes execute on behalf of groups and roles, organizations may require unique identification of individuals in 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 multi-factor 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 accesses). 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-8.

Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts (IA-2(1))

Description for Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts (IA-2(1))
Implement multi-factor authentication for access to privileged accounts.

Discussion for Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts (IA-2(1))
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 such as a cryptographic private key), or something you are (e.g., a biometric). Multi-factor authentication solutions that feature physical authenticators include hardware authenticators that provide time-based or challenge-response outputs and smart cards such as the U.S. Government Personal Identity Verification (PIV) card or the Department of Defense (DoD) Common Access Card (CAC). In addition to authenticating users at the system level (i.e., at logon), organizations may employ authentication mechanisms at the application level, at their discretion, to provide increased security. Regardless of the type of access (i.e., 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.

Identification and Authentication (organizational Users) | Multi-factor Authentication to Non-privileged Accounts (IA-2(2))

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

Discussion for Identification and Authentication (organizational Users) | Multi-factor Authentication to Non-privileged Accounts (IA-2(2))
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 such as a cryptographic private key), or something you are (e.g., a biometric). Multi-factor authentication solutions that feature physical authenticators include hardware authenticators that provide time-based or challenge-response outputs and smart cards such as the U.S. Government Personal Identity Verification card or the DoD Common Access Card. In addition to authenticating users at the system level, organizations may also employ authentication mechanisms at the application level, at their discretion, to provide increased information security. Regardless of the type of access (i.e., local, network, remote), non-privileged accounts are authenticated using multi-factor options appropriate for the level of risk. Organizations can provide additional security measures, such as additional or more rigorous authentication mechanisms, for specific types of access.

Identification and Authentication (organizational Users) | Remote Access — Separate Device (IA-2(11))

Description for Identification and Authentication (organizational Users) | Remote Access — Separate Device (IA-2(11))
[Withdrawn: Incorporated into IA-2(6).]

Discussion for Identification and Authentication (organizational Users) | Remote Access — Separate Device (IA-2(11))

Identification and Authentication (organizational Users) | Local Access to Privileged Accounts (IA-2(3))

Description for Identification and Authentication (organizational Users) | Local Access to Privileged Accounts (IA-2(3))
[Withdrawn: Incorporated into IA-2(1).]

Discussion for Identification and Authentication (organizational Users) | Local Access to Privileged Accounts (IA-2(3))

Identification and Authentication (organizational Users) | Individual Authentication with Group Authentication (IA-2(5))

Description for Identification and Authentication (organizational Users) | Individual Authentication with Group Authentication (IA-2(5))
When shared accounts or authenticators are employed, require users to be individually authenticated before granting access to the shared accounts or resources.

Discussion for Identification and Authentication (organizational Users) | Individual Authentication with Group Authentication (IA-2(5))
Individual authentication prior to shared group authentication mitigates the risk of using group accounts or authenticators.

Identification and Authentication (organizational Users) | Access to Accounts — separate Device (IA-2(6))

Description for Identification and Authentication (organizational Users) | Access to Accounts —separate Device (IA-2(6))
Implement multi-factor authentication for [Selection (one or more): local; network; remote] access to [Selection (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: organization-defined strength of mechanism requirements].

Discussion for Identification and Authentication (organizational Users) | Access to Accounts —separate Device (IA-2(6))
The purpose of requiring a device that is separate from the system 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 authenticators or credentials stored on the system. Adversaries may be able to compromise such authenticators or credentials and subsequently impersonate authorized users. Implementing one of the factors on a separate device (e.g., a hardware token), provides a greater strength of mechanism and an increased level of assurance in the authentication process.

Identification and Authentication (organizational Users) | Local Access to Non-privileged Accounts (IA-2(4))

Description for Identification and Authentication (organizational Users) | Local Access to Non-privileged Accounts (IA-2(4))
[Withdrawn: Incorporated into IA-2(2).]

Discussion for Identification and Authentication (organizational Users) | Local Access to Non-privileged Accounts (IA-2(4))

Identification and Authentication (organizational Users) | Access to Accounts — Replay Resistant (IA-2(8))

Description for Identification and Authentication (organizational Users) | Access to Accounts — Replay Resistant (IA-2(8))
Implement replay-resistant authentication mechanisms for access to [Selection (one or more): privileged accounts; non-privileged accounts].

Discussion for Identification and Authentication (organizational Users) | Access to Accounts — Replay Resistant (IA-2(8))
Authentication processes resist replay attacks if it is impractical to achieve successful authentications by replaying previous authentication messages. Replay-resistant techniques include protocols that use nonces or challenges such as time synchronous or cryptographic authenticators.

Identification and Authentication (organizational Users) | Network Access to Non-privileged Accounts — Separate Device (IA-2(7))

Description for Identification and Authentication (organizational Users) | Network Access to Non-privileged Accounts — Separate Device (IA-2(7))
[Withdrawn: Incorporated into IA-2(6).]

Discussion for Identification and Authentication (organizational Users) | Network Access to Non-privileged Accounts — Separate Device (IA-2(7))

Identification and Authentication (organizational Users) | Single Sign-on (IA-2(10))

Description for Identification and Authentication (organizational Users) | Single Sign-on (IA-2(10))
Provide a single sign-on capability for [Assignment: organization-defined system accounts and services].

Discussion for Identification and Authentication (organizational Users) | Single Sign-on (IA-2(10))
Single sign-on enables users to log in once and gain access to multiple system resources. Organizations consider the operational efficiencies provided by single sign-on capabilities with the risk introduced by allowing access to multiple systems via a single authentication event. Single sign-on can present opportunities to improve system security, for example by providing the ability to add multi-factor authentication for applications and systems (existing and new) that may not be able to natively support multi-factor authentication.

Identification and Authentication (organizational Users) | Network Access to Non-privileged Accounts — Replay Resistant (IA-2(9))

Description for Identification and Authentication (organizational Users) | Network Access to Non-privileged Accounts — Replay Resistant (IA-2(9))
[Withdrawn: Incorporated into IA-2(8).]

Discussion for Identification and Authentication (organizational Users) | Network Access to Non-privileged Accounts — Replay Resistant (IA-2(9))

Identification and Authentication (organizational Users) | Acceptance of PIV Credentials (IA-2(12))

Description for Identification and Authentication (organizational Users) | Acceptance of PIV Credentials (IA-2(12))
Accept and electronically verify Personal Identity Verification-compliant credentials.

Discussion for Identification and Authentication (organizational Users) | Acceptance of PIV Credentials (IA-2(12))
Acceptance of Personal Identity Verification (PIV)-compliant credentials applies to organizations implementing logical access control and physical access control systems. PIV-compliant credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents. The adequacy and reliability of PIV card issuers are authorized using SP 800-79-2. Acceptance of PIV-compliant credentials includes derived PIV credentials, the use of which is addressed in SP 800-166. The DOD Common Access Card (CAC) is an example of a PIV credential.

Identification and Authentication (organizational Users) | Out-of-band Authentication (IA-2(13))

Description for Identification and Authentication (organizational Users) | Out-of-band Authentication (IA-2(13))
Implement the following out-of-band authentication mechanisms under [Assignment: organization-defined conditions]: [Assignment: organization-defined out-of-band authentication].

Discussion for Identification and Authentication (organizational Users) | Out-of-band Authentication (IA-2(13))
Out-of-band authentication refers to the use of two separate communication paths to identify and authenticate users or devices to an information system. The first path (i.e., the in-band path) is used to identify and authenticate users or devices and is generally the path through which information flows. The second path (i.e., the out-of-band path) is used to independently verify the authentication and/or requested action. For example, a user authenticates via a notebook computer to a remote server to which the user desires access and requests some action of the server via that communication path. Subsequently, the server contacts the user via the user's cell phone to verify that the requested action originated from the user. The user may confirm the intended action to an individual on the telephone or provide an authentication code via the telephone. Out-of-band authentication can be used to mitigate actual or suspected man-in the-middle attacks. The conditions or criteria for activation include suspicious activities, new threat indicators, elevated threat levels, or the impact or classification level of information in requested transactions.

Device Identification and Authentication (IA-3)

Description for Device Identification and Authentication (IA-3)
Uniquely identify and authenticate [Assignment: organization-defined devices and/or types of devices] before establishing a [Selection (one or more): local; remote; network] connection.

Discussion for Device Identification and Authentication (IA-3)
Devices that require unique device-to-device identification and authentication are defined by type, device, or a combination of type and device. Organization-defined device types include devices that are not owned by the organization. Systems use shared known information (e.g., Media Access Control [MAC], Transmission Control Protocol/Internet Protocol [TCP/IP] addresses) for device identification or organizational authentication solutions (e.g., Institute of Electrical and Electronics Engineers (IEEE) 802.1x and Extensible Authentication Protocol [EAP], RADIUS server with EAP-Transport Layer Security [TLS] authentication, Kerberos) to identify and authenticate devices on local and wide area networks. Organizations determine the required strength of authentication mechanisms based on the security categories of systems and mission or business requirements. Because of the challenges of implementing device authentication on a large scale, organizations can restrict the application of the control to a limited number/type of devices based on mission or business needs.

Device Identification and Authentication | Cryptographic Bidirectional Authentication (IA-3(1))

Description for Device Identification and Authentication | Cryptographic Bidirectional Authentication (IA-3(1))
Authenticate [Assignment: organization-defined devices and/or types of devices] before establishing [Selection (one or more): local; remote; network] connection using bidirectional authentication that is cryptographically based.

Discussion for Device Identification and Authentication | Cryptographic Bidirectional Authentication (IA-3(1))
A local connection is a connection with a device that communicates without the use of a network. A network connection is a connection with a device that communicates through a network. A remote connection is a connection with a device that communicates through an external network. Bidirectional authentication provides stronger protection to validate the identity of other devices for connections that are of greater risk.

Device Identification and Authentication | Cryptographic Bidirectional Network Authentication (IA-3(2))

Description for Device Identification and Authentication | Cryptographic Bidirectional Network Authentication (IA-3(2))
Withdrawn: Incorporated into IA-3(1).]

Discussion for Device Identification and Authentication | Cryptographic Bidirectional Network Authentication (IA-3(2))

Device Identification and Authentication | Dynamic Address Allocation (IA-3(3))

Description for Device Identification and Authentication | Dynamic Address Allocation (IA-3(3))
(a) Where addresses are allocated dynamically, standardize dynamic address allocation lease information and the lease duration assigned to devices in accordance with [Assignment: organization-defined lease information and lease duration]; and
(b) Audit lease information when assigned to a device.

Discussion for Device Identification and Authentication | Dynamic Address Allocation (IA-3(3))
The Dynamic Host Configuration Protocol (DHCP) is an example of a means by which clients can dynamically receive network address assignments.

Device Identification and Authentication | Device Attestation (IA-3(4))

Description for Device Identification and Authentication | Device Attestation (IA-3(4))
Handle device identification and authentication based on attestation by [Assignment: organization-defined configuration management process].

Discussion for Device Identification and Authentication | Device Attestation (IA-3(4))
Device attestation refers to the identification and authentication of a device based on its configuration and known operating state. Device attestation can be determined via a cryptographic hash of the device. If device attestation is the means of identification and authentication, then it is important that patches and updates to the device are handled via a configuration management process such that the patches and updates are done securely and do not disrupt identification and authentication to other devices.

Identifier Management (IA-4)

Description for Identifier Management (IA-4)
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. Selecting an identifier that identifies an individual, group, role, service, or device;
c. Assigning the identifier to the intended individual, group, role, service, or device; and
d. Preventing reuse of identifiers for [Assignment: organization-defined time period].

Discussion for Identifier Management (IA-4)
Common device identifiers include Media Access Control (MAC) addresses, Internet Protocol (IP) addresses, or device-unique token identifiers. The management of individual identifiers is not applicable to shared system accounts. Typically, individual identifiers are the usernames of the system accounts assigned to those individuals. In such instances, the account management activities of AC-2 use account names provided by IA-4. Identifier management also addresses individual identifiers not necessarily associated with system accounts. Preventing the reuse of identifiers implies preventing the assignment of previously used individual, group, role, service, or device identifiers to different individuals, groups, roles, services, or devices.

Identifier Management | Prohibit Account Identifiers as Public Identifiers (IA-4(1))

Description for Identifier Management | Prohibit Account Identifiers as Public Identifiers (IA-4(1))
Prohibit the use of system account identifiers that are the same as public identifiers for individual accounts.

Discussion for Identifier Management | Prohibit Account Identifiers as Public Identifiers (IA-4(1))
Prohibiting account identifiers as public identifiers applies to any publicly disclosed account identifier used for communication such as, electronic mail and instant messaging. Prohibiting the use of systems account identifiers that are the same as some public identifier, such as the individual identifier section of an electronic mail address, makes it more difficult for adversaries to guess user identifiers.
Prohibiting account identifiers as public identifiers without the implementation of other supporting controls only complicates guessing of identifiers. Additional protections are required for authenticators and credentials to protect the account.

Identifier Management | Supervisor Authorization (IA-4(2))

Description for Identifier Management | Supervisor Authorization (IA-4(2))
[Withdrawn: Incorporated into IA-12(1).]

Discussion for Identifier Management | Supervisor Authorization (IA-4(2))

Identifier Management | Multiple Forms of Certification (IA-4(3))

Description for Identifier Management | Multiple Forms of Certification (IA-4(3))
[Withdrawn: Incorporated into IA-12(2).]

Discussion for Identifier Management | Multiple Forms of Certification (IA-4(3))

Identifier Management | Identify User Status (IA-4(4))

Description for Identifier Management | Identify User Status (IA-4(4))
Manage individual identifiers by uniquely identifying each individual as [Assignment: organization-defined characteristic identifying individual status].

Discussion for Identifier Management | Identify User Status (IA-4(4))
Characteristics that identify the status of individuals include contractors, foreign nationals, and non-organizational users. Identifying the status of individuals by these 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 one of the individuals on an email message is a contractor.

Identifier Management | Dynamic Management (IA-4(5))

Description for Identifier Management | Dynamic Management (IA-4(5))
Manage individual identifiers dynamically in accordance with [Assignment: organization-defined dynamic identifier policy].

Discussion for Identifier Management | Dynamic Management (IA-4(5))
In contrast to conventional approaches to identification that presume static accounts for preregistered users, many distributed systems establish identifiers at runtime for entities that were previously unknown. When identifiers are established at runtime for previously unknown entities, organizations can anticipate and provision for the dynamic establishment of identifiers. Pre-established trust relationships and mechanisms with appropriate authorities to validate credentials and related identifiers are essential.

Identifier Management | Cross-organization Management (IA-4(6))

Description for Identifier Management | Cross-organization Management (IA-4(6))
Coordinate with the following external organizations for cross-organization management of identifiers: [Assignment: organization-defined external organizations].

Discussion for Identifier Management | Cross-organization Management (IA-4(6))
Cross-organization identifier management provides the capability to identify individuals, groups, roles, or devices when conducting cross-organization activities involving the processing, storage, or transmission of information.

Identifier Management | In-person Registration (IA-4(7))

Description for Identifier Management | In-person Registration (IA-4(7))
[Withdrawn: Incorporated into IA-12(4).]

Discussion for Identifier Management | In-person Registration (IA-4(7))

Identifier Management | Pairwise Pseudonymous Identifiers (IA-4(8))

Description for Identifier Management | Pairwise Pseudonymous Identifiers (IA-4(8))
Generate pairwise pseudonymous identifiers.

Discussion for Identifier Management | Pairwise Pseudonymous Identifiers (IA-4(8))
A pairwise pseudonymous identifier is an opaque unguessable subscriber identifier generated by an identity provider for use at a specific individual relying party. Generating distinct pairwise pseudonymous identifiers with no identifying information about a subscriber discourages subscriber activity tracking and profiling beyond the operational requirements established by an organization. The pairwise pseudonymous identifiers are unique to each relying party except in situations where relying parties can show a demonstrable relationship justifying an

operational need for correlation, or all parties consent to being correlated in such a manner.

Identifier Management | Attribute Maintenance and Protection (IA-4(9))

Description for Identifier Management | Attribute Maintenance and Protection (IA-4(9))
Maintain the attributes for each uniquely identified individual, device, or service in [Assignment: organization-defined protected central storage].

Discussion for Identifier Management | Attribute Maintenance and Protection (IA-4(9))
For each of the entities covered in IA-2, IA-3, IA-8, and IA-9, it is important to maintain the attributes for each authenticated entity on an ongoing basis in a central (protected) store.

Authenticator Management (IA-5)

Description for Authenticator Management (IA-5)
Manage system authenticators by:
a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator;
b. Establishing initial authenticator content for any authenticators issued by the organization;
c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators;
e. Changing default authenticators prior to first use;
f. Changing or refreshing authenticators [Assignment: organization-defined time period by authenticator type] or when [Assignment: organization-defined events] occur;
g. Protecting authenticator content from unauthorized disclosure and modification;
h. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; and
i. Changing authenticators for group or role accounts when membership to those accounts changes.

Discussion for Authenticator Management (IA-5)
Authenticators include passwords, cryptographic devices, biometrics, certificates, one-time password devices, and ID badges. Device authenticators include certificates and passwords. Initial authenticator content is the actual content of the authenticator (e.g., the initial password). In contrast, the requirements for authenticator content contain specific criteria or characteristics (e.g., minimum password length). Developers may deliver system components with factory default authentication credentials (i.e., passwords) to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant risk. The requirement to protect individual authenticators may be implemented via control PL-4 or PS-6 for authenticators in the possession of individuals and by controls AC-3, AC-6, and SC-28 for authenticators stored in organizational systems, including passwords 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 rejections 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 immediately reporting lost, stolen, or compromised authenticators. Authenticator management includes issuing and revoking authenticators for temporary access when no longer needed.

Authenticator Management | Password-based Authentication (IA-5(1))

Description for Authenticator Management | Password-based Authentication (IA-5(1))
For password-based authentication:
(a) Maintain a list of commonly-used, expected, or compromised passwords and update the list [Assignment: organization-defined frequency] and when organizational passwords are suspected to have been compromised directly or indirectly;
(b) Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5(1)(a);
(c) Transmit passwords only over cryptographically-protected channels;
(d) Store passwords using an approved salted key derivation function, preferably using a keyed hash;
(e) Require immediate selection of a new password upon account recovery;
(f) Allow user selection of long passwords and passphrases, including spaces and all printable characters;
(g) Employ automated tools to assist the user in selecting strong password authenticators; and
(h) Enforce the following composition and complexity rules: [Assignment: organization-defined composition and complexity rules].

Discussion for Authenticator Management | Password-based Authentication (IA-5(1))
Password-based authentication applies to passwords regardless of whether they are used in single-factor or multi-factor authentication. Long passwords or passphrases are preferable over shorter passwords. Enforced composition rules provide marginal security benefits while decreasing usability. However, organizations may choose to establish certain rules for password generation (e.g., minimum character length for long passwords) under certain circumstances and can enforce this requirement in IA-5(1)(h). Account recovery can occur, for example, in situations when a password is forgotten. Cryptographically protected passwords include salted one-way cryptographic hashes of passwords. The list of commonly used, compromised, or expected passwords includes passwords obtained from previous breach corpuses, dictionary words, and repetitive or sequential characters. The list includes context-specific words, such as the name of the service, username, and derivatives thereof.

Authenticator Management | Public Key-based Authentication (IA-5(2))

Description for Authenticator Management | Public Key-based Authentication (IA-5(2))
(a) For public key-based authentication:
(1) Enforce authorized access to the corresponding private key; and
(2) Map the authenticated identity to the account of the individual or group; and
(b) When public key infrastructure (PKI) is used:
(1) Validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information; and
(2) Implement a local cache of revocation data to support path discovery and validation.

Discussion for Authenticator Management | Public Key-based Authentication (IA-5(2))
Public key cryptography is a valid authentication mechanism for individuals, machines, and devices. For PKI solutions, status information for certification paths includes certificate revocation lists or certificate status protocol responses. For PIV cards, certificate validation involves the construction and verification of a certification path to the Common Policy Root trust anchor, which includes certificate policy processing. Implementing a local cache of revocation data to support path discovery and validation also supports system availability in situations where organizations are unable to access revocation information via the network.

Authenticator Management | Hardware Token-based Authentication (IA-5(11))

Description for Authenticator Management | Hardware Token-based Authentication (IA-5(11))
[Withdrawn: Incorporated into IA-2(1) and IA-2(2).]

Discussion for Authenticator Management | Hardware Token-based Authentication (IA-5(11))

Authenticator Management | In-person or Trusted External Party Registration (IA-5(3))

Description for Authenticator Management | In-person or Trusted External Party Registration (IA-5(3))
[Withdrawn: Incorporated into IA-12(4).]

Discussion for Authenticator Management | In-person or Trusted External Party Registration (IA-5(3))

Authenticator Management | Change Authenticators Prior to Delivery (IA-5(5))

Description for Authenticator Management | Change Authenticators Prior to Delivery (IA-5(5))
Require developers and installers of system components to provide unique authenticators or change default authenticators prior to delivery and installation.

Discussion for Authenticator Management | Change Authenticators Prior to Delivery (IA-5(5))
Changing authenticators prior to the 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 authenticators or change default authenticators for system components prior to delivery and/or installation. However, it typically does not apply to developers of commercial off-the-shelf information technology products.

Requirements for unique authenticators can be included in acquisition documents prepared by organizations when procuring systems or system components.

Authenticator Management | Protection of Authenticators (IA-5(6))

Description for Authenticator Management | Protection of Authenticators (IA-5(6))
Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access.

Discussion for Authenticator Management | Protection of Authenticators (IA-5(6))
For systems that contain multiple security categories of information without reliable physical or logical separation between categories, authenticators used to grant access to the systems are protected commensurate with the highest security category of information on the systems. Security categories of information are determined as part of the security categorization process.

Authenticator Management | No Embedded Unencrypted Static Authenticators (IA-5(7))

Description for Authenticator Management | No Embedded Unencrypted Static Authenticators (IA-5(7))
Ensure that unencrypted static authenticators are not embedded in applications or other forms of static storage.

Discussion for Authenticator Management | No Embedded Unencrypted Static Authenticators (IA-5(7))
In addition to applications, other forms of static storage include access scripts and function keys. Organizations exercise caution when determining whether embedded or stored authenticators are in encrypted or unencrypted form. If authenticators are used in the manner stored, then those representations are considered unencrypted authenticators.

Authenticator Management | Multiple System Accounts (IA-5(8))

Description for Authenticator Management | Multiple System Accounts (IA-5(8))
Implement [Assignment: organization-defined security controls] to manage the risk of compromise due to individuals having accounts on multiple systems.

Discussion for Authenticator Management | Multiple System Accounts (IA-5(8))
When individuals have accounts on multiple systems and use the same authenticators such as passwords, there is the risk that a compromise of one account may lead to the compromise of other accounts. Alternative approaches include having different authenticators (passwords) on all systems, employing a single sign-on or federation mechanism, or using some form of one-time passwords on all systems. Organizations can also use rules of behavior (see PL-4) and access agreements (see PS-6) to mitigate the risk of multiple system accounts.

Authenticator Management | Federated Credential Management (IA-5(9))

Description for Authenticator Management | Federated Credential Management (IA-5(9))
Use the following external organizations to federate credentials: [Assignment: organization-defined external organizations].

Discussion for Authenticator Management | Federated Credential Management (IA-5(9))
Federation provides organizations with the capability to authenticate individuals and devices when conducting cross-organization activities involving the processing, storage, or transmission of information. Using a specific list of approved external organizations for authentication helps to ensure that those organizations are vetted and trusted.

Authenticator Management | Dynamic Credential Binding (IA-5(10))

Description for Authenticator Management | Dynamic Credential Binding (IA-5(10))
Bind identities and authenticators dynamically using the following rules: [Assignment: organization-defined binding rules].

Discussion for Authenticator Management | Dynamic Credential Binding (IA-5(10))
Authentication requires some form of binding between an identity and the authenticator that is used to confirm the identity. In conventional approaches, binding is established by pre-provisioning both the identity and the authenticator to the system. For example, the binding between a username (i.e., identity) and a password (i.e., authenticator) is accomplished by provisioning the identity and authenticator as a pair in the system. New authentication techniques allow the binding between the identity and the authenticator to be implemented external to a system. For example, with smartcard credentials, the identity and authenticator are bound together on the smartcard. Using these credentials, systems can authenticate identities that have not been pre-provisioned, dynamically provisioning the identity after authentication. In these situations, organizations can anticipate the dynamic provisioning of identities. Pre-established trust relationships and mechanisms with appropriate authorities to validate identities and related credentials are essential.

Authenticator Management | Automated Support for Password Strength Determination (IA-5(4))

Description for Authenticator Management | Automated Support for Password Strength Determination (IA-5(4))
[Withdrawn: Incorporated into IA-5(1).]

Discussion for Authenticator Management | Automated Support for Password Strength Determination (IA-5(4))

Authenticator Management | Biometric Authentication Performance (IA-5(12))

Description for Authenticator Management | Biometric Authentication Performance (IA-5(12))
For biometric-based authentication, employ mechanisms that satisfy the following biometric quality requirements [Assignment: organization-defined biometric quality requirements].

Discussion for Authenticator Management | Biometric Authentication Performance (IA-5(12))
Unlike password-based authentication, which provides exact matches of user-input passwords to stored passwords, biometric authentication does not provide exact matches. Depending on the type of biometric and the type of collection mechanism, there is likely to be some divergence from the presented biometric and the stored biometric that serves as the basis for comparison. Matching performance is the rate at which a biometric algorithm correctly results in a match for a genuine user and rejects other users. Biometric performance requirements include the match rate, which reflects the accuracy of the biometric matching algorithm used by a system.

Authenticator Management | Expiration of Cached Authenticators (IA-5(13))

Description for Authenticator Management | Expiration of Cached Authenticators (IA-5(13))
Prohibit the use of cached authenticators after [Assignment: organization-defined time period].

Discussion for Authenticator Management | Expiration of Cached Authenticators (IA-5(13))
Cached authenticators are used to authenticate to the local machine when the network is not available. If cached authentication information is out of date, the validity of the authentication information may be questionable.

Authenticator Management | Managing Content of PKI Trust Stores (IA-5(14))

Description for Authenticator Management | Managing Content of PKI Trust Stores (IA-5(14))
For PKI-based authentication, employ an organization-wide methodology for managing the content of PKI trust stores installed across all platforms, including networks, operating systems, browsers, and applications.

Discussion for Authenticator Management | Managing Content of PKI Trust Stores (IA-5(14))
An organization-wide methodology for managing the content of PKI trust stores helps improve the accuracy and currency of PKI-based authentication credentials across the organization.

Authenticator Management | GSA-approved Products and Services (IA-5(15))

Description for Authenticator Management | GSA-approved Products and Services (IA-5(15))
Use only General Services Administration-approved products and services for identity, credential, and access management.

Discussion for Authenticator Management | GSA-approved Products and Services (IA-5(15))
General Services Administration (GSA)-approved products and services are products and services that have been approved through the GSA conformance program, where applicable, and posted to the GSA Approved Products List. GSA provides guidance for teams to design and build functional and secure systems that comply with Federal Identity, Credential, and Access Management (FICAM) policies, technologies, and implementation patterns.

Authenticator Management | In-person or Trusted External Party Authenticator Issuance (IA-5(16))

Description for Authenticator Management | In-person or Trusted External Party Authenticator Issuance (IA-5(16))
Require that the issuance of [Assignment: organization-defined types of and/or specific authenticators] be conducted [Selection: in person; by a trusted external party] before [Assignment: organization-defined registration authority] with authorization by [Assignment: organization-defined personnel or roles].

Discussion for Authenticator Management | In-person or Trusted External Party Authenticator Issuance (IA-5(16))
Issuing authenticators in person or by a trusted external party enhances and reinforces the trustworthiness of the identity proofing process.

Authenticator Management | Presentation Attack Detection for Biometric Authenticators (IA-5(17))

Description for Authenticator Management | Presentation Attack Detection for Biometric Authenticators (IA-5(17))
Employ presentation attack detection mechanisms for biometric-based authentication.

Discussion for Authenticator Management | Presentation Attack Detection for Biometric Authenticators (IA-5(17))
Biometric characteristics do not constitute secrets. Such characteristics can be obtained by online web accesses, taking a picture of someone with a camera phone to obtain facial images with or without their knowledge, lifting from objects that someone has touched (e.g., a latent fingerprint), or capturing a high-resolution image (e.g., an iris pattern). Presentation attack detection technologies including liveness detection, can mitigate the risk of these types of attacks by making it difficult to produce artifacts intended to defeat the biometric sensor.

Authenticator Management | Password Managers (IA-5(18))

Description for Authenticator Management | Password Managers (IA-5(18))
(a) Employ [Assignment: organization-defined password managers] to generate and manage passwords; and
(b) Protect the passwords using [Assignment: organization-defined controls].

Discussion for Authenticator Management | Password Managers (IA-5(18))
For systems where static passwords are employed, it is often a challenge to ensure that the passwords are suitably complex and that the same passwords are not employed on multiple systems. A password manager is a solution to this problem as it automatically generates and stores strong and different passwords for various accounts. A potential risk of using password managers is that adversaries can target the collection of passwords generated by the password manager. Therefore, the collection of passwords requires protection including encrypting the passwords (see IA-5(1)(d)) and storing the collection offline in a token.

Authentication Feedback (IA-6)

Description for Authentication Feedback (IA-6)
Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.

Discussion for Authentication Feedback (IA-6)
Authentication feedback from systems does not provide information that would allow unauthorized individuals to compromise authentication mechanisms. For some types of systems, such as desktops or notebooks with relatively large monitors, the threat (referred to as shoulder surfing) may be significant. For other types of systems, such as mobile devices with small displays, the threat may be less significant and is balanced against the increased likelihood of typographic input errors due to small keyboards. Thus, the means for obscuring authentication feedback is selected accordingly. Obscuring authentication feedback includes displaying asterisks when users type passwords into input devices or displaying feedback for a very limited time before obscuring it.

Cryptographic Module Authentication (IA-7)

Description for Cryptographic Module Authentication (IA-7)
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.

Discussion for Cryptographic Module Authentication (IA-7)
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.

Identification and Authentication (non-organizational Users) (IA-8)

Description for Identification and Authentication (non-organizational Users) (IA-8)
Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.

Discussion for Identification and Authentication (non-organizational Users) (IA-8)
Non-organizational users include system users other than organizational users explicitly covered by IA-2. Non-organizational users are uniquely identified and authenticated for accesses other than those explicitly identified and documented in AC-14. 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—when balancing the need to ensure ease of use for access to federal information and systems with the need to protect and adequately mitigate risk.

Identification and Authentication (non-organizational Users) | Acceptance of PIV Credentials from Other Agencies (IA-8(1))

Description for Identification and Authentication (non-organizational Users) | Acceptance of PIV Credentials from Other Agencies (IA-8(1))
Accept and electronically verify Personal Identity Verification-compliant credentials from other federal agencies.

Discussion for Identification and Authentication (non-organizational Users) | Acceptance of PIV Credentials from Other Agencies (IA-8(1))
Acceptance of Personal Identity Verification (PIV) credentials from other federal agencies applies 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.

Identification and Authentication (non-organizational Users) | Acceptance of External Authenticators (IA-8(2))

Description for Identification and Authentication (non-organizational Users) | Acceptance of External Authenticators (IA-8(2))
(a) Accept only external authenticators that are NIST-compliant; and
(b) Document and maintain a list of accepted external authenticators.

Discussion for Identification and Authentication (non-organizational Users) | Acceptance of External Authenticators (IA-8(2))
Acceptance of only NIST-compliant external authenticators applies to organizational systems that are accessible to the public (e.g., public-facing websites). External authenticators are issued by nonfederal government entities and are compliant with SP 800-63B. Approved external authenticators meet or exceed the minimum Federal Government-wide technical, security, privacy, and organizational maturity requirements. Meeting or exceeding Federal requirements allows Federal Government relying parties to trust external authenticators in connection with an authentication transaction at a specified authenticator assurance level.

Identification and Authentication (non-organizational Users) | Use of FICAM-approved Products (IA-8(3))

Description for Identification and Authentication (non-organizational Users) | Use of FICAM-approved Products (IA-8(3))
[Withdrawn: Incorporated into IA-8(2).]

Discussion for Identification and Authentication (non-organizational Users) | Use of FICAM-approved Products (IA-8(3))

Identification and Authentication (non-organizational Users) | Use of Defined Profiles (IA-8(4))

Description for Identification and Authentication (non-organizational Users) | Use of Defined Profiles (IA-8(4))
Conform to the following profiles for identity management [Assignment: organization-defined identity management profiles].

Discussion for Identification and Authentication (non-organizational Users) | Use of Defined Profiles (IA-8(4))
Organizations define profiles for identity management based on open identity management standards. To ensure that open identity management standards are viable, robust, reliable, sustainable, and interoperable as documented, the Federal Government assesses and scopes the standards and technology implementations against applicable laws, executive orders, directives, policies, regulations, standards, and guidelines.

Identification and Authentication (non-organizational Users) | Acceptance of PVI-I Credentials (IA-8(5))

Description for Identification and Authentication (non-organizational Users) | Acceptance of PVI-I Credentials (IA-8(5))
Accept and verify federated or PKI credentials that meet [Assignment: organization-defined policy].

Discussion for Identification and Authentication (non-organizational Users) | Acceptance of PVI-I Credentials (IA-8(5))
Acceptance of PIV-I credentials can be implemented by PIV, PIV-I, and other commercial or external identity providers. The acceptance and verification of PIV-I-compliant credentials apply to both logical and physical access control systems. The acceptance and verification of PIV-I credentials address nonfederal issuers of identity cards that desire to interoperate with United States Government PIV systems and that can be trusted by Federal Government-relying parties. The X.509 certificate policy for the Federal Bridge Certification Authority (FBCA) addresses PIV-I requirements. The PIV-I card is commensurate with the PIV credentials as defined in cited references. PIV-I credentials are the credentials issued by a PIV-I provider whose PIV-I certificate policy maps to the Federal Bridge PIV-I Certificate Policy. A PIV-I provider is cross-certified with the FBCA (directly or through another PKI bridge) with policies that have been mapped and approved as meeting the requirements of the PIV-I policies defined in the FBCA certificate policy.

Identification and Authentication (non-organizational Users) | Disassociability (IA-8(6))

Description for Identification and Authentication (non-organizational Users) | Disassociability (IA-8(6))
Implement the following measures to disassociate user attributes or identifier assertion relationships among individuals, credential service providers, and relying parties: [Assignment: organization-defined measures].

Discussion for Identification and Authentication (non-organizational Users) | Disassociability (IA-8(6))
Federated identity solutions can create increased privacy risks due to the tracking and profiling of individuals. Using identifier mapping tables or cryptographic techniques to blind credential service providers and relying parties from each other or to make identity attributes less visible to transmitting parties can reduce these privacy risks.

Service Identification and Authentication (IA-9)

Description for Service Identification and Authentication (IA-9)
Uniquely identify and authenticate [Assignment: organization-defined system services and applications] before establishing communications with devices, users, or other services or applications.

Discussion for Service Identification and Authentication (IA-9)
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 and applications include information or code signing, provenance graphs, and electronic signatures that indicate the sources of services. Decisions regarding the validity of identification and authentication claims can be made by services separate from the services acting on those decisions. This can occur in distributed system architectures. In such situations, the identification and authentication

decisions (instead of actual identifiers and authentication data) are provided to the services that need to act on those decisions.

Service Identification and Authentication | Information Exchange (IA-9(1))

Description for Service Identification and Authentication | Information Exchange (IA-9(1))
[Withdrawn: Incorporated into IA-9.]

Discussion for Service Identification and Authentication | Information Exchange (IA-9(1))

Service Identification and Authentication | Transmission of Decisions (IA-9(2))

Description for Service Identification and Authentication | Transmission of Decisions (IA-9(2))
[Withdrawn: Incorporated into IA-9.]

Discussion for Service Identification and Authentication | Transmission of Decisions (IA-9(2))

Adaptive Authentication (IA-10)

Description for Adaptive Authentication (IA-10)
Require individuals accessing the system to employ [Assignment: organization-defined supplemental authentication techniques or mechanisms] under specific [Assignment: organization-defined circumstances or situations].

Discussion for Adaptive Authentication (IA-10)
Adversaries may compromise individual authentication mechanisms employed by organizations and subsequently attempt to impersonate 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 quantities of information than individuals would routinely access; or attempting to access information from suspicious network addresses. When pre-established conditions or triggers 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 or types of records being accessed. Adaptive authentication does not replace and is not used to avoid the use of multi-factor authentication mechanisms but can augment implementations of multi-factor authentication.

Re-authentication (IA-11)

Description for Re-authentication (IA-11)
Require users to re-authenticate when [Assignment: organization-defined circumstances or situations requiring re-authentication].

Discussion for Re-authentication (IA-11)
In addition to the re-authentication requirements associated with device locks, organizations may require re-authentication of individuals in certain situations, including when roles, authenticators or credentials change, when security categories of systems change, when the execution of privileged functions occurs, after a fixed time period, or periodically.

Identity Proofing (IA-12)

Description for Identity Proofing (IA-12)
a. Identity proof users that require accounts for 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.

Discussion for Identity Proofing (IA-12)
Identity proofing is the process of collecting, validating, and verifying a user's identity information for the purposes of establishing credentials for accessing a system. 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 800-63-3 and SP 800-63A. Organizations may be subject to laws, executive orders, directives, regulations, or policies that address the collection of identity evidence. Organizational personnel consult with the senior agency official for privacy and legal counsel regarding such requirements.

Identity Proofing | Supervisor Authorization (IA-12(1))

Description for Identity Proofing | Supervisor Authorization (IA-12(1))
Require that the registration process to receive an account for logical access includes supervisor or sponsor authorization.

Discussion for Identity Proofing | Supervisor Authorization (IA-12(1))
Including supervisor or sponsor authorization as part of the registration process provides an additional level of scrutiny to ensure that the user's management chain 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.

Identity Proofing | Identity Evidence (IA-12(2))

Description for Identity Proofing | Identity Evidence (IA-12(2))
Require evidence of individual identification be presented to the registration authority.

Discussion for Identity Proofing | Identity Evidence (IA-12(2))
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 risks to the systems, roles, and privileges associated with the user's account.

Identity Proofing | Identity Evidence Validation and Verification (IA-12(3))

Description for Identity Proofing | Identity Evidence Validation and Verification (IA-12(3))
Require that the presented identity evidence be validated and verified through [Assignment: organizational defined methods of validation and verification].

Discussion for Identity Proofing | Identity Evidence Validation and Verification (IA-12(3))
Validation and verification of identity evidence increases the assurance that accounts and identifiers are being established for the correct user and authenticators are being bound to that user. Validation refers to the process of confirming that the evidence is genuine and authentic, and the data contained in the evidence is correct, current, and related to an individual. Verification confirms and establishes a linkage between the claimed identity and the actual existence of the user presenting the evidence. Acceptable methods for validating and verifying identity evidence are consistent with the risks to the systems, roles, and privileges associated with the users account.

Identity Proofing | In-person Validation and Verification (IA-12(4))

Description for Identity Proofing | In-person Validation and Verification (IA-12(4))
Require that the validation and verification of identity evidence be conducted in person before a designated registration authority.

Discussion for Identity Proofing | In-person Validation and Verification (IA-12(4))
In-person proofing reduces the likelihood of fraudulent credentials being issued because it requires the physical presence of individuals, the presentation of physical identity documents, and actual face-to-face interactions with designated registration authorities.

Identity Proofing | Address Confirmation (IA-12(5))

Description for Identity Proofing | Address Confirmation (IA-12(5))
Require that a [Selection: registration code; notice of proofing] be delivered through an out-of-band channel to verify the users address (physical or digital) of record.

Discussion for Identity Proofing | Address Confirmation (IA-12(5))
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 ensure that the individual associated with an address of record is the same individual that participated in the registration. Confirmation can take the form of a temporary enrollment code or a notice of proofing. The delivery address for these artifacts is obtained from records and not self-asserted 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.

Identity Proofing | Accept Externally-proofed Identities (IA-12(6))

Description for Identity Proofing | Accept Externally-proofed Identities (IA-12(6))
Accept externally-proofed identities at [Assignment: organization-defined identity assurance level].

Discussion for Identity Proofing | Accept Externally-proofed Identities (IA-12(6))
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 the identity assurance level appropriate for the system, application, or information accessed. Accepting externally-proofed identities is a fundamental component of managing federated identities across agencies and organizations.

Policy and Procedures (IR-1)

Description for Policy and Procedures (IR-1)
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] incident response policy that:
(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
(b) Is consistent with applicable laws, executive 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;
b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the incident response policy and procedures; and
c. Review and update the current incident response:
1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

Discussion for Policy and Procedures (IR-1)
Incident response policy and procedures address the controls in the IR family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of incident response policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, 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. Events that may precipitate an update to incident response policy and procedures include assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Incident Response Training (IR-2)

Description for Incident Response Training (IR-2)
a. Provide incident response training to system users consistent with assigned roles and responsibilities:
1. Within [Assignment: organization-defined time period] of assuming an incident response role or responsibility or acquiring system access;
2. When required by system changes; and
3. [Assignment: organization-defined frequency] thereafter; and
b. Review and update incident response training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

Discussion for Incident Response Training (IR-2)
Incident response training is associated with the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail are 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 incident responders may receive more specific training on forensics, 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. Events that may precipitate an update to incident response training content include, but are not limited to, incident response plan testing or response to an actual incident (lessons learned), assessment or audit findings, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Incident Response Training | Simulated Events (IR-2(1))

Description for Incident Response Training | Simulated Events (IR-2(1))
Incorporate simulated events into incident response training to facilitate the required response by personnel in crisis situations.

Discussion for Incident Response Training | Simulated Events (IR-2(1))
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.

Incident Response Training | Automated Training Environments (IR-2(2))

Description for Incident Response Training | Automated Training Environments (IR-2(2))
Provide an incident response training environment using [Assignment: organization-defined automated mechanisms].

Discussion for Incident Response Training | Automated Training Environments (IR-2(2))
Automated mechanisms can provide a more thorough and realistic incident response training environment. This can be accomplished, for example, by providing more complete coverage of incident response issues, selecting more realistic training scenarios and environments, and stressing the response capability.

Incident Response Training | Breach (IR-2(3))

Description for Incident Response Training | Breach (IR-2(3))
Provide incident response training on how to identify and respond to a breach, including the organization's process for reporting a breach.

Discussion for Incident Response Training | Breach (IR-2(3))
For federal agencies, an incident that involves personally identifiable information is considered a breach. 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 authorized user accesses or potentially accesses such information for other than authorized purposes. The incident response training emphasizes the obligation of individuals to report both confirmed and suspected breaches involving information in any medium or form, including paper, oral, and electronic. Incident response training includes tabletop exercises that simulate a breach. See IR-2(1).

Incident Response Testing (IR-3)

Description for Incident Response Testing (IR-3)
Test the effectiveness of the incident response capability for the system [Assignment: organization-defined frequency] using the following tests: [Assignment: organization-defined tests].

Discussion for Incident Response Testing (IR-3)
Organizations test incident response capabilities to determine their effectiveness and identify potential weaknesses or deficiencies. Incident response testing includes the use of checklists, walk-through or tabletop exercises, and simulations (parallel or full interrupt). Incident response testing can include a determination of the effects on organizational operations and assets and individuals due to incident response. The use of qualitative and quantitative data aids in determining the effectiveness of incident response processes.

Incident Response Testing | Automated Testing (IR-3(1))

Description for Incident Response Testing | Automated Testing (IR-3(1))
Test the incident response capability using [Assignment: organization-defined automated mechanisms].

Discussion for Incident Response Testing | Automated Testing (IR-3(1))
Organizations use automated mechanisms to more thoroughly and effectively test incident response capabilities. This can be accomplished by providing more complete coverage of incident response issues, selecting realistic test scenarios and environments, and stressing the response capability.

Incident Response Testing | Coordination with Related Plans (IR-3(2))

Description for Incident Response Testing | Coordination with Related Plans (IR-3(2))
Coordinate incident response testing with organizational elements responsible for related plans.

Discussion for Incident Response Testing | Coordination with Related Plans (IR-3(2))
Organizational plans related to incident response testing include business continuity plans, disaster recovery plans, continuity of operations plans, contingency plans, crisis communications plans, critical infrastructure plans, and occupant emergency plans.

Incident Response Testing | Continuous Improvement (IR-3(3))

Description for Incident Response Testing | Continuous Improvement (IR-3(3))
Use qualitative and quantitative data from testing to:
(a) Determine the effectiveness of incident response processes;
(b) Continuously improve incident response processes; and
(c) Provide incident response measures and metrics that are accurate, consistent, and in a reproducible format.

Discussion for Incident Response Testing | Continuous Improvement (IR-3(3))
To help incident response activities function as intended, organizations may use metrics and evaluation criteria to assess incident response programs as part of an effort to continually improve response performance. These efforts facilitate improvement in incident response efficacy and lessen the impact of incidents.

Incident Handling (IR-4)

Description for Incident Handling (IR-4)
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; and
d. Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.

Discussion for Incident Handling (IR-4)
Organizations recognize that incident response capabilities are dependent on the capabilities of organizational systems and the mission and business processes being supported by those systems. Organizations consider incident response as part of the definition, design, and development of mission and 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. An effective incident handling capability includes coordination among many organizational entities (e.g., mission or business owners, system owners, authorizing officials, human resources offices, physical security offices, personnel security offices, legal departments, risk executive [function], operations personnel, procurement offices). Suspected security incidents include the receipt of suspicious email 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. For federal agencies, an

incident that involves personally identifiable information is considered a breach. A breach results in unauthorized disclosure, the loss of control, unauthorized acquisition, compromise, or a similar occurrence where a person other than an authorized user accesses or potentially accesses personally identifiable information or an authorized user accesses or potentially accesses such information for other than authorized purposes.

Incident Handling | Automated Incident Handling Processes (IR-4(1))

Description for Incident Handling | Automated Incident Handling Processes (IR-4(1))
Support the incident handling process using [Assignment: organization-defined automated mechanisms].

Discussion for Incident Handling | Automated Incident Handling Processes (IR-4(1))
Automated mechanisms that support incident handling processes include online incident management systems and tools that support the collection of live response data, full network packet capture, and forensic analysis.

Incident Handling | Dynamic Reconfiguration (IR-4(2))

Description for Incident Handling | Dynamic Reconfiguration (IR-4(2))
Include the following types of dynamic reconfiguration for [Assignment: organization-defined system components] as part of the incident response capability: [Assignment: organization-defined types of dynamic reconfiguration].

Discussion for Incident Handling | Dynamic Reconfiguration (IR-4(2))
Dynamic reconfiguration includes changes to router rules, access control lists, intrusion detection or prevention system parameters, and filter rules for guards or firewalls. Organizations may perform dynamic reconfiguration of systems to stop attacks, misdirect attackers, and isolate components of systems, thus limiting the extent of the damage from breaches or compromises. Organizations include specific time frames for achieving the reconfiguration of systems in the definition

of the reconfiguration capability, considering the potential need for rapid response to effectively address cyber threats.

Incident Handling | Continuity of Operations (IR-4(3))

Description for Incident Handling | Continuity of Operations (IR-4(3))
Identify [Assignment: organization-defined classes of incidents] and take the following actions in response to those incidents to ensure continuation of organizational mission and business functions: [Assignment: organization-defined actions to take in response to classes of incidents].

Discussion for Incident Handling | Continuity of Operations (IR-4(3))
Classes of incidents include malfunctions due to design or implementation errors and omissions, targeted malicious attacks, and untargeted malicious attacks. Incident response actions include orderly system degradation, system shutdown, fall back to manual mode or activation of alternative technology whereby the system operates differently, employing deceptive 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 as part of IR-4(5).

Incident Handling | Information Correlation (IR-4(4))

Description for Incident Handling | Information Correlation (IR-4(4))
Correlate incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.

Discussion for Incident Handling | Information Correlation (IR-4(4))
Sometimes, a threat event, such as a hostile cyber-attack, can only be observed by bringing together information from different sources, including various reports and reporting procedures established by organizations.

Incident Handling | Automatic Disabling of System (IR-4(5))

Description for Incident Handling | Automatic Disabling of System (IR-4(5))
Implement a configurable capability to automatically disable the system if [Assignment: organization-defined security violations] are detected.

Discussion for Incident Handling | Automatic Disabling of System (IR-4(5))
Organizations consider whether the capability to automatically disable the system conflicts with continuity of operations requirements specified as part of CP-2 or IR-4(3). Security violations include cyber-attacks that have compromised the integrity of the system or exfiltrated organizational information and serious errors in software programs that could adversely impact organizational missions or functions or jeopardize the safety of individuals.

Incident Handling | Insider Threats (IR-4(6))

Description for Incident Handling | Insider Threats (IR-4(6))
Implement an incident handling capability for incidents involving insider threats.

Discussion for Incident Handling | Insider Threats (IR-4(6))
Explicit focus on handling incidents involving insider threats provides additional emphasis on this type of threat and the need for specific incident handling capabilities to provide appropriate and timely responses.

Incident Handling | Insider Threats — Intra-organization Coordination (IR-4(7))

Description for Incident Handling | Insider Threats — Intra-organization Coordination (IR-4(7))
Coordinate an incident handling capability for insider threats that includes the following organizational entities [Assignment: organization-defined entities].

Discussion for Incident Handling | Insider Threats — Intra-organization Coordination (IR-4(7))
Incident handling for insider threat incidents (e.g., preparation, detection and analysis, containment, eradication, and recovery) requires coordination among many organizational entities, including mission or business owners, system owners, human resources offices, procurement offices, personnel offices, physical security offices, 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.

Incident Handling | Correlation with External Organizations (IR-4(8))

Description for Incident Handling | Correlation with External Organizations (IR-4(8))
Coordinate with [Assignment: organization-defined external organizations] to correlate and share [Assignment: organization-defined incident information] to achieve a cross-organization perspective on incident awareness and more effective incident responses.

Discussion for Incident Handling | Correlation with External Organizations (IR-4(8))
The coordination of incident information with external organizations—including mission or business partners, military or coalition partners, customers, and developers—can provide significant benefits. Cross-organizational coordination can serve as an important risk management capability. This capability allows organizations to leverage information from a variety of sources to effectively respond to incidents and breaches that could potentially affect the organization's operations, assets, and individuals.

Incident Handling | Dynamic Response Capability (IR-4(9))

Description for Incident Handling | Dynamic Response Capability (IR-4(9))
Employ [Assignment: organization-defined dynamic response capabilities] to respond to incidents.

Discussion for Incident Handling | Dynamic Response Capability (IR-4(9))
The 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.

Incident Handling | Supply Chain Coordination (IR-4(10))

Description for Incident Handling | Supply Chain Coordination (IR-4(10))
Coordinate incident handling activities involving supply chain events with other organizations involved in the supply chain.

Discussion for Incident Handling | Supply Chain Coordination (IR-4(10))
Organizations involved in supply chain activities include product developers, system integrators, manufacturers, packagers, assemblers, distributors, vendors, and resellers. Supply chain incidents can occur anywhere through or to the supply chain and include compromises or breaches that involve primary or sub-tier providers, information technology products, system components, development processes or personnel, and distribution processes or warehousing facilities. Organizations consider including processes for protecting and sharing incident information in information exchange agreements and their obligations for reporting incidents to government oversight bodies (e.g., Federal Acquisition Security Council).

Incident Handling | Integrated Incident Response Team (IR-4(11))

Description for Incident Handling | Integrated Incident Response Team (IR-4(11))
Establish and maintain an integrated incident response team that can be deployed to any location identified by the organization in [Assignment: organization-defined time period].

Discussion for Incident Handling | Integrated Incident Response Team (IR-4(11))
An integrated incident response team is a team of experts that assesses, documents, and responds to incidents so that organizational systems and networks can recover quickly and implement the necessary controls to avoid future incidents. Incident response team personnel include forensic and malicious code analysts, tool developers, systems security and privacy engineers, and real-time operations personnel. The incident handling capability includes performing rapid forensic preservation of evidence and analysis of and response to intrusions. For some organizations, the incident response team can be a cross-organizational entity.
An integrated incident response team facilitates information sharing and allows organizational personnel (e.g., developers, implementers, and operators) to leverage team knowledge of the threat and implement defensive measures that enable organizations to deter intrusions more effectively. Moreover, integrated teams promote the rapid detection of intrusions, the development of appropriate mitigations, and the deployment of effective defensive measures. For example, when an intrusion is detected, the integrated team can rapidly develop an appropriate response for operators to implement, correlate the new incident with information on past intrusions, and augment ongoing cyber intelligence development. Integrated incident response teams are better able to identify

adversary tactics, techniques, and procedures that are linked to the operations tempo or specific mission and business functions and to define responsive actions in a way that does not disrupt those mission and business functions. Incident response teams can be distributed within organizations to make the capability resilient.

Incident Handling | Malicious Code and Forensic Analysis (IR-4(12))

Description for Incident Handling | Malicious Code and Forensic Analysis (IR-4(12))
Analyze malicious code and/or other residual artifacts remaining in the system after the incident.

Discussion for Incident Handling | Malicious Code and Forensic Analysis (IR-4(12))
When conducted carefully in an isolated environment, analysis of malicious code and other residual artifacts of a security incident or breach can give the organization insight into adversary tactics, techniques, and procedures. It can also indicate the identity or some defining characteristics of the adversary. In addition, malicious code analysis can help the organization develop responses to future incidents.

Incident Handling | Behavior Analysis (IR-4(13))

Description for Incident Handling | Behavior Analysis (IR-4(13))
Analyze anomalous or suspected adversarial behavior in or related to [Assignment: organization-defined environments or resources].

Discussion for Incident Handling | Behavior Analysis (IR-4(13))
If the organization maintains a deception environment, an analysis of behaviors in that environment, including resources targeted by the adversary and timing of the incident or event, can provide insight into adversarial tactics, techniques, and procedures. External to a deception environment, the analysis of anomalous adversarial behavior (e.g., changes in system performance or usage patterns) or suspected behavior (e.g., changes in searches for the location of specific resources) can give the organization such insight.

Incident Handling | Security Operations Center (IR-4(14))

Description for Incident Handling | Security Operations Center (IR-4(14))
Establish and maintain a security operations center.

Discussion for Incident Handling | Security Operations Center (IR-4(14))
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 defend and monitor an organization's systems and networks (i.e., 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 controls (including monitoring, scanning, and forensics tools) to monitor, fuse, correlate, analyze, and respond to threat and security-relevant event data from multiple sources. These sources 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 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 a capability.

Incident Handling | Public Relations and Reputation Repair (IR-4(15))

Description for Incident Handling | Public Relations and Reputation Repair (IR-4(15))
(a) Manage public relations associated with an incident; and
(b) Employ measures to repair the reputation of the organization.

Discussion for Incident Handling | Public Relations and Reputation Repair (IR-4(15))
It is important for an organization to have a strategy in place for addressing incidents that have been brought to the attention of the general public, have cast the organization in a negative light, or have affected the organization's constituents (e.g., partners, customers). Such publicity can be extremely harmful to the organization and affect its ability to carry out its mission and business functions. Taking proactive steps to repair the organization's reputation is an essential aspect of reestablishing the trust and confidence of its constituents.

Incident Monitoring (IR-5)

Description for Incident Monitoring (IR-5)
Track and document incidents.

Discussion for Incident Monitoring (IR-5)
Documenting incidents includes maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics as well as 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 complaints, supply chain partners, audit monitoring, physical access monitoring, and user and administrator reports. IR-4 provides information on the types of incidents that are appropriate for monitoring.

Incident Monitoring | Automated Tracking, Data Collection, and Analysis (IR-5(1))

Description for Incident Monitoring | Automated Tracking, Data Collection, and Analysis (IR-5(1))
Track incidents and collect and analyze incident information using [Assignment: organization-defined automated mechanisms].

Discussion for Incident Monitoring | Automated Tracking, Data Collection, and Analysis (IR-5(1))
Automated mechanisms for tracking incidents and collecting and analyzing incident information include Computer Incident Response Centers or other electronic databases of incidents and network monitoring devices.

Incident Reporting (IR-6)

Description for Incident Reporting (IR-6)
a. Require personnel to report suspected incidents to the organizational incident response capability within [Assignment: organization-defined time period]; and
b. Report incident information to [Assignment: organization-defined authorities].

Discussion for Incident Reporting (IR-6)
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. Incident information can inform risk assessments, control effectiveness assessments, security requirements for acquisitions, and selection criteria for technology products.

Incident Reporting | Automated Reporting (IR-6(1))

Description for Incident Reporting | Automated Reporting (IR-6(1))
Report incidents using [Assignment: organization-defined automated mechanisms].

Discussion for Incident Reporting | Automated Reporting (IR-6(1))
The recipients of incident reports are specified in IR-6b. Automated reporting mechanisms include email, posting on websites (with automatic updates), and automated incident response tools and programs.

Incident Reporting | Vulnerabilities Related to Incidents (IR-6(2))

Description for Incident Reporting | Vulnerabilities Related to Incidents (IR-6(2))
Report system vulnerabilities associated with reported incidents to [Assignment: organization-defined personnel or roles].

Discussion for Incident Reporting | Vulnerabilities Related to Incidents (IR-6(2))
Reported incidents that uncover system vulnerabilities are analyzed by organizational personnel including system owners, mission and business owners, senior agency information security officers, senior agency officials for privacy, authorizing officials, and the risk executive (function). The analysis can serve to prioritize and initiate mitigation actions to address the discovered system vulnerability.

Incident Reporting | Supply Chain Coordination (IR-6(3))

Description for Incident Reporting | Supply Chain Coordination (IR-6(3))
Provide incident information to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident.

Discussion for Incident Reporting | Supply Chain Coordination (IR-6(3))
Organizations involved in supply chain activities include product developers, system integrators, manufacturers, packagers, assemblers, distributors, vendors, and resellers. Entities that provide supply chain governance include the Federal Acquisition Security Council (FASC). Supply chain incidents include compromises or breaches that involve information technology products, system components, development processes or personnel, distribution processes, or warehousing facilities. Organizations determine the appropriate information to share and consider the value gained from informing external organizations about supply

chain incidents, including the ability to improve processes or to identify the root cause of an incident.

Incident Response Assistance (IR-7)

Description for Incident Response Assistance (IR-7)
Provide an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the system for the handling and reporting of incidents.

Discussion for Incident Response Assistance (IR-7)
Incident response support resources provided by organizations include help desks, assistance groups, automated ticketing systems to open and track incident response tickets, and access to forensics services or consumer redress services, when required.

Incident Response Assistance | Automation Support for Availability of Information and Support (IR-7(1))

Description for Incident Response Assistance | Automation Support for Availability of Information and Support (IR-7(1))
Increase the availability of incident response information and support using [Assignment: organization-defined automated mechanisms].

Discussion for Incident Response Assistance | Automation Support for Availability of Information and Support (IR-7(1))
Automated mechanisms can 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 increasing understanding of current response capabilities and support.

Incident Response Assistance | Coordination with External Providers (IR-7(2))

Description for Incident Response Assistance | Coordination with External Providers (IR-7(2))
(a) Establish a direct, cooperative relationship between its incident response capability and external providers of system protection capability; and
(b) Identify organizational incident response team members to the external providers.

Discussion for Incident Response Assistance | Coordination with External Providers (IR-7(2))
External providers of a 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.

Incident Response Plan (IR-8)

Description for Incident Response Plan (IR-8)
a. Develop an incident response plan that:
1. Provides the organization with a roadmap for implementing its incident response capability;
2. Describes the structure and organization of the incident response capability;
3. Provides a high-level approach for how the incident response capability fits into the overall organization;
4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
5. Defines reportable incidents;
6. Provides metrics for measuring the incident response capability within the organization;
7. Defines the resources and management support needed to effectively maintain and mature an incident response capability;
8. Addresses the sharing of incident information;
9. Is reviewed and approved by [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency]; and
10. Explicitly designates responsibility for incident response to [Assignment: organization-defined entities, personnel, or roles].
b. Distribute copies of the incident response plan to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements];
c. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing;
d. Communicate incident response plan changes to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; and
e. Protect the incident response plan from unauthorized disclosure and modification.

Discussion for Incident Response Plan (IR-8)
It is important that organizations develop and implement a coordinated approach to incident response. Organizational mission and business functions determine the structure of incident response capabilities. As part of the incident response capabilities, organizations consider the coordination and sharing of information with external organizations, including external service providers and other organizations involved in the supply chain. For incidents involving personally identifiable information (i.e., breaches), include a process to determine whether notice to oversight organizations or affected individuals is appropriate and provide that notice accordingly.

Incident Response Plan | Breaches (IR-8(1))

Description for Incident Response Plan | Breaches (IR-8(1))
Include the following in the Incident Response Plan for breaches involving personally identifiable information:
(a) A process to determine if notice to individuals or other organizations, including oversight organizations, is needed;
(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.

Discussion for Incident Response Plan | Breaches (IR-8(1))
Organizations may be required by law, regulation, or policy to follow specific procedures relating to breaches, including notice to individuals, affected organizations, and oversight bodies; standards of harm; and mitigation or other specific requirements.

Information Spillage Response (IR-9)

Description for Information Spillage Response (IR-9)
Respond to information spills by:
a. Assigning [Assignment: organization-defined personnel or roles] with responsibility for responding to information spills;
b. Identifying the specific information involved in the system contamination;
c. Alerting [Assignment: organization-defined personnel or roles] of the information spill using a method of communication not associated with the spill;
d. Isolating the contaminated system or system 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. Performing the following additional actions: [Assignment: organization-defined actions].

Discussion for Information Spillage Response (IR-9)
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 a higher classification or impact level. At that point, corrective action is required. The nature of the response is based on the classification or impact level of the spilled information, the security capabilities of the system, the specific nature of the contaminated 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 contamination is isolated and eradicated.

Integrated Information Security Analysis Team (IR-10)

Description for Integrated Information Security Analysis Team (IR-10)
[Withdrawn: Moved to IR-4(11).]

Discussion for Integrated Information Security Analysis Team (IR-10)

Information Spillage Response | Training (IR-9(2))

Description for Information Spillage Response | Training (IR-9(2))
Provide information spillage response training [Assignment: organization-defined frequency].

Discussion for Information Spillage Response | Training (IR-9(2))
Organizations 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.

Information Spillage Response | Post-spill Operations (IR-9(3))

Description for Information Spillage Response | Post-spill Operations (IR-9(3))
Implement the following procedures to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions: [Assignment: organization-defined procedures].

Discussion for Information Spillage Response | Post-spill Operations (IR-9(3))
Corrective actions for systems contaminated due to information spillages 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.

Information Spillage Response | Exposure to Unauthorized Personnel (IR-9(4))

Description for Information Spillage Response | Exposure to Unauthorized Personnel (IR-9(4))
Employ the following controls for personnel exposed to information not within assigned access authorizations: [Assignment: organization-defined controls].

Discussion for Information Spillage Response | Exposure to Unauthorized Personnel (IR-9(4))
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.

Information Spillage Response | Responsible Personnel (IR-9(1))

Description for Information Spillage Response | Responsible Personnel (IR-9(1))
[Withdrawn: Incorporated into IR-9.]

Discussion for Information Spillage Response | Responsible Personnel (IR-9(1))

Policy and Procedures (MA-1)

Description for Policy and Procedures (MA-1)
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] maintenance policy that:
(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the maintenance policy and the associated maintenance controls;
b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the maintenance policy and procedures; and
c. Review and update the current maintenance:
1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

Discussion for Policy and Procedures (MA-1)
Maintenance policy and procedures address the controls in the MA family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of maintenance policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, 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. Events that may precipitate an update to maintenance policy and procedures assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Controlled Maintenance (MA-2)

Description for Controlled Maintenance (MA-2)
a. Schedule, document, and review records of maintenance, repair, and replacement on system components in accordance with manufacturer or vendor specifications and/or organizational requirements;
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;
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;
d. Sanitize equipment to remove the following information from associated media prior to removal from organizational facilities for off-site maintenance, repair, or replacement: [Assignment: organization-defined information];
e. Check all potentially impacted controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions; and
f. Include the following information in organizational maintenance records: [Assignment: organization-defined information].

Discussion for Controlled Maintenance (MA-2)
Controlling 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, copiers, and printers. Information necessary for creating effective maintenance records includes the date and time of maintenance, a description of the maintenance performed, names of the individuals or group performing the maintenance, name of the escort, and system components or equipment that are removed or replaced. Organizations consider supply chain-related risks associated with replacement components for systems.

Controlled Maintenance | Record Content (MA-2(1))

Description for Controlled Maintenance | Record Content (MA-2(1))
[Withdrawn: Incorporated into MA-2.]

Discussion for Controlled Maintenance | Record Content (MA-2(1))

Controlled Maintenance | Automated Maintenance Activities (MA-2(2))

Description for Controlled Maintenance | Automated Maintenance Activities (MA-2(2))
(a) Schedule, conduct, and document maintenance, repair, and replacement actions for the system using [Assignment: organization-defined automated mechanisms]; and
(b) Produce up-to date, accurate, and complete records of all maintenance, repair, and replacement actions requested, scheduled, in process, and completed.

Discussion for Controlled Maintenance | Automated Maintenance Activities (MA-2(2))
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.

Maintenance Tools (MA-3)

Description for Maintenance Tools (MA-3)
a. Approve, control, and monitor the use of system maintenance tools; and
b. Review previously approved system maintenance tools [Assignment: organization-defined frequency].

Discussion for Maintenance Tools (MA-3)
Approving, controlling, monitoring, and reviewing maintenance tools address security-related issues associated with maintenance tools that are not within system authorization boundaries and are used specifically for diagnostic and repair actions on organizational systems. Organizations have flexibility in determining roles for the approval of maintenance tools and how that approval is documented. A periodic review of maintenance tools facilitates the withdrawal of approval for outdated, unsupported, irrelevant, or no-longer-used tools. Maintenance tools can include hardware, software, and firmware items and may be pre-installed, brought in with maintenance personnel on media, cloud-based, or downloaded from a website. Such tools can be vehicles for transporting malicious code, either intentionally or unintentionally, into a facility and subsequently into systems. Maintenance tools can include hardware and software diagnostic test equipment and packet sniffers. The hardware and software components that support maintenance and are a part of the system (including the software implementing utilities such as ping, ls, ipconfig, or the hardware and software implementing the monitoring port of an Ethernet switch) are not addressed by maintenance tools.

Maintenance Tools | Inspect Tools (MA-3(1))

Description for Maintenance Tools | Inspect Tools (MA-3(1))
Inspect the maintenance tools used by maintenance personnel for improper or unauthorized modifications.

Discussion for Maintenance Tools | Inspect Tools (MA-3(1))
Maintenance tools can be directly brought into a facility by maintenance personnel or downloaded from a vendor's website. If, upon inspection of the maintenance tools, organizations determine that the tools have been modified in an improper manner or the tools contain malicious code, the incident is handled consistent with organizational policies and procedures for incident handling.

Maintenance Tools | Inspect Media (MA-3(2))

Description for Maintenance Tools | Inspect Media (MA-3(2))
Check media containing diagnostic and test programs for malicious code before the media are used in the system.

Discussion for Maintenance Tools | Inspect Media (MA-3(2))
If, upon inspection of media containing maintenance, diagnostic, and test programs, organizations determine that the media contains malicious code, the incident is handled consistent with organizational incident handling policies and procedures.

Maintenance Tools | Prevent Unauthorized Removal (MA-3(3))

Description for Maintenance Tools | Prevent Unauthorized Removal (MA-3(3))
Prevent the removal of maintenance equipment containing organizational information by:
(a) Verifying that there is no organizational information contained on the equipment;
(b) Sanitizing or destroying the equipment;
(c) Retaining the equipment within the facility; or
(d) Obtaining an exemption from [Assignment: organization-defined personnel or roles] explicitly authorizing removal of the equipment from the facility.

Discussion for Maintenance Tools | Prevent Unauthorized Removal (MA-3(3))
Organizational information includes all information owned by organizations and any information provided to organizations for which the organizations serve as information stewards.

Maintenance Tools | Restricted Tool Use (MA-3(4))

Description for Maintenance Tools | Restricted Tool Use (MA-3(4))
Restrict the use of maintenance tools to authorized personnel only.

Discussion for Maintenance Tools | Restricted Tool Use (MA-3(4))
Restricting the use of maintenance tools to only authorized personnel applies to systems that are used to carry out maintenance functions.

Maintenance Tools | Execution with Privilege (MA-3(5))

Description for Maintenance Tools | Execution with Privilege (MA-3(5))
Monitor the use of maintenance tools that execute with increased privilege.

Discussion for Maintenance Tools | Execution with Privilege (MA-3(5))
Maintenance tools that execute with increased system privilege can result in unauthorized access to organizational information and assets that would otherwise be inaccessible.

Maintenance Tools | Software Updates and Patches (MA-3(6))

Description for Maintenance Tools | Software Updates and Patches (MA-3(6))
Inspect maintenance tools to ensure the latest software updates and patches are installed.

Discussion for Maintenance Tools | Software Updates and Patches (MA-3(6))
Maintenance tools using outdated and/or unpatched software can provide a threat vector for adversaries and result in a significant vulnerability for organizations.

Nonlocal Maintenance (MA-4)

Description for Nonlocal Maintenance (MA-4)
a. Approve and monitor nonlocal maintenance and diagnostic activities;
b. Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system;
c. Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions;
d. Maintain records for nonlocal maintenance and diagnostic activities; and
e. Terminate session and network connections when nonlocal maintenance is completed.

Discussion for Nonlocal Maintenance (MA-4)
Nonlocal maintenance and diagnostic activities are conducted by individuals who communicate through either an external or internal network. Local maintenance and diagnostic activities are carried out by individuals who are physically present at the system location and not communicating across a network connection. Authentication techniques used to establish nonlocal maintenance and diagnostic sessions reflect the network access requirements in IA-2. Strong authentication requires authenticators that are resistant to replay attacks and employ multi-factor authentication. Strong authenticators include PKI where certificates are stored on a token protected by a password, passphrase, or biometric. Enforcing requirements in MA-4 is accomplished, in part, by other controls. SP 800-63B provides additional guidance on strong authentication and authenticators.

Nonlocal Maintenance | Logging and Review (MA-4(1))

Description for Nonlocal Maintenance | Logging and Review (MA-4(1))
(a) Log [Assignment: organization-defined audit events] for nonlocal maintenance and diagnostic sessions; and
(b) Review the audit records of the maintenance and diagnostic sessions to detect anomalous behavior.

Discussion for Nonlocal Maintenance | Logging and Review (MA-4(1))
Audit logging for nonlocal maintenance is enforced by AU-2. Audit events are defined in AU-2a.

Nonlocal Maintenance | Document Nonlocal Maintenance (MA-4(2))

Description for Nonlocal Maintenance | Document Nonlocal Maintenance (MA-4(2))
[Withdrawn: Incorporated into MA-1 and MA-4.]

Discussion for Nonlocal Maintenance | Document Nonlocal Maintenance (MA-4(2))

Nonlocal Maintenance | Comparable Security and Sanitization (MA-4(3))

Description for Nonlocal Maintenance | Comparable Security and Sanitization (MA-4(3))
(a) Require that nonlocal maintenance and diagnostic services be performed from a system that implements a security capability comparable to the capability implemented on the system being serviced; or
(b) Remove the component to be serviced from the system prior to nonlocal maintenance or diagnostic services; sanitize the component (for organizational information); and after the service is performed, inspect and sanitize the component (for potentially malicious software) before reconnecting the component to the system.

Discussion for Nonlocal Maintenance | Comparable Security and Sanitization (MA-4(3))
Comparable security capability on systems, diagnostic tools, and equipment providing maintenance services implies that the implemented controls on those systems, tools, and equipment are at least as comprehensive as the controls on the system being serviced.

Nonlocal Maintenance | Authentication and Separation of Maintenance Sessions (MA-4(4))

Description for Nonlocal Maintenance | Authentication and Separation of Maintenance Sessions (MA-4(4))
Protect nonlocal maintenance sessions by:
(a) Employing [Assignment: organization-defined authenticators that are replay resistant]; and
(b) Separating the maintenance sessions from other network sessions with the system by either:
(1) Physically separated communications paths; or
(2) Logically separated communications paths.

Discussion for Nonlocal Maintenance | Authentication and Separation of Maintenance Sessions (MA-4(4))
Communications paths can be logically separated using encryption.

Nonlocal Maintenance | Approvals and Notifications (MA-4(5))

Description for Nonlocal Maintenance | Approvals and Notifications (MA-4(5))
(a) Require the approval of each nonlocal maintenance session by [Assignment: organization-defined personnel or roles]; and
(b) Notify the following personnel or roles of the date and time of planned nonlocal maintenance: [Assignment: organization-defined personnel or roles].

Discussion for Nonlocal Maintenance | Approvals and Notifications (MA-4(5))
Notification may be performed by maintenance personnel. Approval of nonlocal maintenance is accomplished by personnel with sufficient information security and system knowledge to determine the appropriateness of the proposed maintenance.

Nonlocal Maintenance | Cryptographic Protection (MA-4(6))

Description for Nonlocal Maintenance | Cryptographic Protection (MA-4(6))
Implement the following cryptographic mechanisms to protect the integrity and confidentiality of nonlocal maintenance and diagnostic communications: [Assignment: organization-defined cryptographic mechanisms].

Discussion for Nonlocal Maintenance | Cryptographic Protection (MA-4(6))
Failure to protect nonlocal maintenance and diagnostic communications can result in unauthorized individuals gaining access to organizational information. Unauthorized access during remote maintenance sessions can result in a variety of hostile actions, including malicious code insertion, unauthorized changes to system parameters, and exfiltration of organizational information. Such actions can result in the loss or degradation of mission or business capabilities.

Nonlocal Maintenance | Disconnect Verification (MA-4(7))

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

Discussion for Nonlocal Maintenance | Disconnect Verification (MA-4(7))
Verifying the termination of a connection once maintenance is completed ensures that connections established during nonlocal maintenance and diagnostic sessions have been terminated and are no longer available for use.

Maintenance Personnel (MA-5)

Description for Maintenance Personnel (MA-5)
a. Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel;
b. Verify that non-escorted personnel performing maintenance on the system possess the required access authorizations; and
c. Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

Discussion for Maintenance Personnel (MA-5)
Maintenance personnel refers to individuals who perform hardware or software maintenance on organizational systems, while PE-2 addresses physical access for individuals whose maintenance duties place them within the physical protection perimeter of the systems. Technical competence of supervising individuals relates to the maintenance performed on the systems, while having required access authorizations refers to maintenance on and near the systems. Individuals not previously identified as authorized maintenance personnel—such as information technology manufacturers, vendors, systems integrators, and consultants—may require privileged access to organizational systems, such as when they are required to conduct maintenance activities with little or no notice. Based on organizational assessments of risk, organizations may issue temporary credentials to these individuals. Temporary credentials may be for one-time use or for very limited time periods.

Maintenance Personnel | Individuals Without Appropriate Access (MA-5(1))

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

Discussion for Maintenance Personnel | Individuals Without Appropriate Access (MA-5(1))
Procedures for individuals who lack appropriate security clearances or who are not U.S. citizens are intended to deny visual and electronic access to classified or controlled unclassified information contained on organizational systems. Procedures for the use of maintenance personnel can be documented in security plans for the systems.

Maintenance Personnel | Security Clearances for Classified Systems (MA-5(2))

Description for Maintenance Personnel | Security Clearances for Classified Systems (MA-5(2))
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.

Discussion for Maintenance Personnel | Security Clearances for Classified Systems (MA-5(2))
Personnel who conduct maintenance on organizational systems may be exposed to classified information during the course of their maintenance activities. To mitigate the inherent risk of such exposure, organizations use maintenance personnel that are cleared (i.e., possess security clearances) to the classification level of the information stored on the system.

Maintenance Personnel | Citizenship Requirements for Classified Systems (MA-5(3))

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

Discussion for Maintenance Personnel | Citizenship Requirements for Classified Systems (MA-5(3))
Personnel who conduct maintenance on organizational systems may be exposed to classified information during the course of their maintenance activities. If access to classified information on organizational systems is restricted to U.S. citizens, the same restriction is applied to personnel performing maintenance on those systems.

Maintenance Personnel | Foreign Nationals (MA-5(4))

Description for Maintenance Personnel | Foreign Nationals (MA-5(4))
Ensure 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 fully documented within Memoranda of Agreements.

Discussion for Maintenance Personnel | Foreign Nationals (MA-5(4))
Personnel who conduct maintenance and diagnostic activities on organizational systems may be exposed to classified information. If non-U.S. citizens are permitted to perform maintenance and diagnostics activities on classified systems, then additional vetting is required to ensure agreements and restrictions are not being violated.

Maintenance Personnel | Non-system Maintenance (MA-5(5))

Description for Maintenance Personnel | Non-system Maintenance (MA-5(5))
Ensure 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.

Discussion for Maintenance Personnel | Non-system Maintenance (MA-5(5))
Personnel who perform maintenance activities in other capacities not directly related to the system include physical plant personnel and custodial personnel.

Timely Maintenance (MA-6)

Description for Timely Maintenance (MA-6)
Obtain maintenance support and/or spare parts for [Assignment: organization-defined system components] within [Assignment: organization-defined time period] of failure.

Discussion for Timely Maintenance (MA-6)
Organizations specify the system components that result in increased risk to organizational operations and assets, individuals, other organizations, or the Nation when the functionality provided by those components is not operational. Organizational actions to obtain maintenance support include having appropriate contracts in place.

Timely Maintenance | Preventive Maintenance (MA-6(1))

Description for Timely Maintenance | Preventive Maintenance (MA-6(1))
Perform preventive maintenance on [Assignment: organization-defined system components] at [Assignment: organization-defined time intervals].

Discussion for Timely Maintenance | Preventive Maintenance (MA-6(1))
Preventive maintenance includes proactive care and the servicing of system components to maintain organizational equipment and facilities in satisfactory operating condition. Such 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 what preventive (or other) failure management policies to apply 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 indications.

Timely Maintenance | Predictive Maintenance (MA-6(2))

Description for Timely Maintenance | Predictive Maintenance (MA-6(2))
Perform predictive maintenance on [Assignment: organization-defined system components] at [Assignment: organization-defined time intervals].

Discussion for Timely Maintenance | Predictive Maintenance (MA-6(2))
Predictive maintenance evaluates the condition of equipment by performing periodic or continuous (online) 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.

Timely Maintenance | Automated Support for Predictive Maintenance (MA-6(3))

Description for Timely Maintenance | Automated Support for Predictive Maintenance (MA-6(3))
Transfer predictive maintenance data to a maintenance management system using [Assignment: organization-defined automated mechanisms].

Discussion for Timely Maintenance | Automated Support for Predictive Maintenance (MA-6(3))
A computerized maintenance management system maintains a database of information about the maintenance operations of organizations and automates the processing of equipment condition data to trigger maintenance planning, execution, and reporting.

Field Maintenance (MA-7)

Description for Field Maintenance (MA-7)
Restrict or prohibit field maintenance on [Assignment: organization-defined systems or system components] to [Assignment: organization-defined trusted maintenance facilities].

Discussion for Field Maintenance (MA-7)
Field maintenance is the type of maintenance conducted on a system or system component after the system or component has been deployed to a specific site (i.e., operational environment). In certain instances, field maintenance (i.e., local maintenance at the site) may not be executed with the same degree of rigor or with the same quality control checks as depot maintenance. For critical systems designated as such by the organization, it may be necessary to restrict or prohibit field maintenance at the local site and require that such maintenance be conducted in trusted facilities with additional controls.

Policy and Procedures (MP-1)

Description for Policy and Procedures (MP-1)
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] media protection policy that:
(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the media protection policy and the associated media protection controls;
b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the media protection policy and procedures; and
c. Review and update the current media protection:
1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

Discussion for Policy and Procedures (MP-1)
Media protection policy and procedures address the controls in the MP family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of media protection policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, 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. Events that may precipitate an update to media protection policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Media Access (MP-2)

Description for Media Access (MP-2)
Restrict access to [Assignment: organization-defined types of digital and/or non-digital media] to [Assignment: organization-defined personnel or roles].

Discussion for Media Access (MP-2)
System media includes digital and non-digital media. Digital media includes flash drives, diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state, magnetic), compact discs, and digital versatile discs. Non-digital media includes paper and microfilm. Denying access to patient medical records in a community hospital unless the individuals 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 discs in the media library to individuals on the system development team is an example of restricting access to digital media.

Media Access | Automated Restricted Access (MP-2(1))

Description for Media Access | Automated Restricted Access (MP-2(1))
[Withdrawn: Incorporated into MP-4(2).]

Discussion for Media Access | Automated Restricted Access (MP-2(1))

Media Access | Cryptographic Protection (MP-2(2))

Description for Media Access | Cryptographic Protection (MP-2(2))
[Withdrawn: Incorporated into SC-28(1).]

Discussion for Media Access | Cryptographic Protection (MP-2(2))

Media Marking (MP-3)

Description for Media Marking (MP-3)
a. Mark system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and
b. Exempt [Assignment: organization-defined types of system media] from marking if the media remain within [Assignment: organization-defined controlled areas].

Discussion for Media Marking (MP-3)
Security marking refers to the application or use of human-readable security attributes. Digital media includes diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state, magnetic), flash drives, compact discs, and digital versatile discs. Non-digital media includes paper and microfilm. Controlled unclassified information is defined by the National Archives and Records Administration along with the appropriate safeguarding and dissemination requirements for such information and is codified in 32 CFR 2002. Security markings are generally not required for media that contains information determined by organizations to be in the public domain or to be publicly releasable. Some organizations may require markings for public information indicating that the information is publicly releasable. System media marking

reflects applicable laws, executive orders, directives, policies, regulations, standards, and guidelines.

Media Storage (MP-4)

Description for Media Storage (MP-4)
a. Physically control and securely store [Assignment: organization-defined types of digital and/or non-digital media] within [Assignment: organization-defined controlled areas]; and
b. Protect system media types defined in MP-4a until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

Discussion for Media Storage (MP-4)
System media includes digital and non-digital media. Digital media includes flash drives, diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state, magnetic), compact discs, and digital versatile discs. Non-digital media includes paper and microfilm. Physically 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. Fewer controls may be needed for media that contains information determined to be in the public domain, publicly releasable, or have limited adverse impacts on organizations, operations, or individuals if accessed by other than authorized personnel. In these situations, physical access controls provide adequate protection.

Media Storage | Cryptographic Protection (MP-4(1))

Description for Media Storage | Cryptographic Protection (MP-4(1))
[Withdrawn: Incorporated into SC-28(1).]

Discussion for Media Storage | Cryptographic Protection (MP-4(1))

Media Storage | Automated Restricted Access (MP-4(2))

Description for Media Storage | Automated Restricted Access (MP-4(2))
Restrict access to media storage areas and log access attempts and access granted using [Assignment: organization-defined automated mechanisms].

Discussion for Media Storage | Automated Restricted Access (MP-4(2))
Automated mechanisms include keypads, biometric readers, or card readers on the external entries to media storage areas.

Media Transport (MP-5)

Description for Media Transport (MP-5)
a. Protect and control [Assignment: organization-defined types of system media] during transport outside of controlled areas using [Assignment: organization-defined controls];
b. Maintain accountability for system media during transport outside of controlled areas;
c. Document activities associated with the transport of system media; and
d. Restrict the activities associated with the transport of system media to authorized personnel.

Discussion for Media Transport (MP-5)
System media includes digital and non-digital media. Digital media includes flash drives, diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state and magnetic), compact discs, and digital versatile 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 processes, and the actual transport. Authorized transport and courier personnel may include individuals external to the organization. Maintaining accountability of media during transport includes restricting transport activities to authorized personnel and tracking and/or obtaining records of transport activities as the media moves through the transportation system to prevent and detect loss, destruction, or tampering. Organizations establish documentation requirements for activities associated with the transport of system media in accordance with organizational assessments of risk. Organizations maintain the flexibility to define record-keeping methods for the different types of media transport as part of a system of transport-related records.

Media Transport | Protection Outside of Controlled Areas (MP-5(1))

Description for Media Transport | Protection Outside of Controlled Areas (MP-5(1))
[Withdrawn: Incorporated into MP-5.]

Discussion for Media Transport | Protection Outside of Controlled Areas (MP-5(1))

Media Transport | Documentation of Activities (MP-5(2))

Description for Media Transport | Documentation of Activities (MP-5(2))
[Withdrawn: Incorporated into MP-5.]

Discussion for Media Transport | Documentation of Activities (MP-5(2))

Media Transport | Custodians (MP-5(3))

Description for Media Transport | Custodians (MP-5(3))
Employ an identified custodian during transport of system media outside of controlled areas.

Discussion for Media Transport | Custodians (MP-5(3))
Identified custodians provide organizations with specific points of contact during the media transport process and facilitate individual accountability. Custodial responsibilities can be transferred from one individual to another if an unambiguous custodian is identified.

Media Transport | Cryptographic Protection (MP-5(4))

Description for Media Transport | Cryptographic Protection (MP-5(4))
[Withdrawn: Incorporated into SC-28(1).]

Discussion for Media Transport | Cryptographic Protection (MP-5(4))

Media Sanitization (MP-6)

Description for Media Sanitization (MP-6)
a. Sanitize [Assignment: organization-defined system media] prior to disposal, release out of organizational control, or release for reuse using [Assignment: organization-defined sanitization techniques and procedures]; and
b. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

Discussion for Media Sanitization (MP-6)
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 in scanners, copiers, printers, notebook computers, workstations, network components, mobile devices, and non-digital media (e.g., 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 erase, 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 methods, recognizing that destruction is sometimes necessary when other methods cannot be applied to media requiring sanitization. Organizations use discretion on the employment of approved sanitization techniques and procedures for media that contains information deemed to be in the public domain or publicly releasable or

information deemed to have no adverse impact on organizations 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. NSA standards and policies control the sanitization process for media that contains classified information. NARA policies control the sanitization process for controlled unclassified information.

Media Sanitization | Review, Approve, Track, Document, and Verify (MP-6(1))

Description for Media Sanitization | Review, Approve, Track, Document, and Verify (MP-6(1))
Review, approve, track, document, and verify media sanitization and disposal actions.

Discussion for Media Sanitization | Review, Approve, Track, Document, and Verify (MP-6(1))
Organizations review and approve media to be sanitized to ensure compliance with records retention policies. Tracking and documenting actions include listing personnel who reviewed and approved sanitization and disposal actions, types of media sanitized, files stored on the media, sanitization methods used, date and time of the sanitization actions, personnel who performed the sanitization, verification actions taken and personnel who performed the verification, and the disposal actions taken. Organizations verify that the sanitization of the media was effective prior to disposal.

Media Sanitization | Equipment Testing (MP-6(2))

Description for Media Sanitization | Equipment Testing (MP-6(2))
Test sanitization equipment and procedures [Assignment: organization-defined frequency] to ensure that the intended sanitization is being achieved.

Discussion for Media Sanitization | Equipment Testing (MP-6(2))
Testing of sanitization equipment and procedures may be conducted by qualified and authorized external entities, including federal agencies or external service providers.

Media Sanitization | Nondestructive Techniques (MP-6(3))

Description for Media Sanitization | Nondestructive Techniques (MP-6(3))
Apply nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the system under the following circumstances: [Assignment: organization-defined circumstances requiring sanitization of portable storage devices].

Discussion for Media Sanitization | Nondestructive Techniques (MP-6(3))
Portable storage devices include external or removable hard disk drives (e.g., solid state, magnetic), optical discs, magnetic or optical tapes, flash memory devices, flash memory cards, and other external or removable disks. Portable storage devices can be obtained from untrustworthy sources and contain malicious code that can be inserted into or transferred to organizational systems through USB ports or other entry portals. While scanning storage devices is recommended, sanitization provides additional assurance that such devices are free of malicious code. Organizations consider nondestructive sanitization of portable storage devices when the devices are purchased from manufacturers or vendors prior to initial use or when organizations cannot maintain a positive chain of custody for the devices.

Media Sanitization | Controlled Unclassified Information (MP-6(4))

Description for Media Sanitization | Controlled Unclassified Information (MP-6(4))
[Withdrawn: Incorporated into MP-6.]

Discussion for Media Sanitization | Controlled Unclassified Information (MP-6(4))

Media Sanitization | Classified Information (MP-6(5))

Description for Media Sanitization | Classified Information (MP-6(5))
[Withdrawn: Incorporated into MP-6.]

Discussion for Media Sanitization | Classified Information (MP-6(5))

Media Sanitization | Media Destruction (MP-6(6))

Description for Media Sanitization | Media Destruction (MP-6(6))
[Withdrawn: Incorporated into MP-6.]

Discussion for Media Sanitization | Media Destruction (MP-6(6))

Media Sanitization | Dual Authorization (MP-6(7))

Description for Media Sanitization | Dual Authorization (MP-6(7))
Enforce dual authorization for the sanitization of [Assignment: organization-defined system media].

Discussion for Media Sanitization | Dual Authorization (MP-6(7))
Organizations employ dual authorization to help ensure that system media sanitization cannot occur unless two technically qualified individuals conduct the designated task. Individuals who sanitize system media possess sufficient skills and expertise to determine if the proposed sanitization reflects applicable federal and organizational standards, policies, and procedures. Dual authorization also helps to ensure that sanitization occurs as intended, protecting against errors and false claims of having performed the sanitization actions. 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.

Media Sanitization | Remote Purging or Wiping of Information (MP-6(8))

Description for Media Sanitization | Remote Purging or Wiping of Information (MP-6(8))
Provide the capability to purge or wipe information from [Assignment: organization-defined systems or system components] [Selection: remotely; under the following conditions: [Assignment: organization-defined conditions]].

Discussion for Media Sanitization | Remote Purging or Wiping of Information (MP-6(8))
Remote purging or wiping of information protects information on organizational systems and system components if systems or components are obtained by unauthorized individuals. Remote purge or wipe commands require strong authentication to help mitigate the risk of unauthorized individuals purging or wiping the system, component, or device. The purge or wipe function can be implemented in a variety of ways, including by overwriting data or information multiple times or by destroying the key necessary to decrypt encrypted data.

Media Use (MP-7)

Description for Media Use (MP-7)
a. [Selection: Restrict; Prohibit] the use of [Assignment: organization-defined types of system media] on [Assignment: organization-defined systems or system components] using [Assignment: organization-defined controls]; and
b. Prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner.

Discussion for Media Use (MP-7)
System media includes both digital and non-digital media. Digital media includes diskettes, magnetic tapes, flash drives, compact discs, digital versatile discs, and removable hard disk drives. Non-digital media includes paper and microfilm. Media use protections also apply to mobile devices with information storage capabilities. In contrast to MP-2, which restricts user access to media, MP-7 restricts the use of certain types of media on systems, for example, restricting or prohibiting the use of flash drives or external hard disk drives. Organizations use technical and nontechnical controls to restrict the use of system media. Organizations may restrict the use of portable storage devices, for example, by using physical cages on workstations to prohibit access to certain external ports or disabling 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, such as by prohibiting the use of writeable, portable storage devices and implementing this restriction by disabling or removing the capability to write to such devices. Requiring identifiable owners for storage devices reduces the risk of using such devices by allowing organizations to assign responsibility for addressing known vulnerabilities in the devices.

Media Use | Prohibit Use Without Owner (MP-7(1))

Description for Media Use | Prohibit Use Without Owner (MP-7(1))
[Withdrawn: Incorporated into MP-7.]

Discussion for Media Use | Prohibit Use Without Owner (MP-7(1))

Media Use | Prohibit Use of Sanitization-resistant Media (MP-7(2))

Description for Media Use | Prohibit Use of Sanitization-resistant Media (MP-7(2))
Prohibit the use of sanitization-resistant media in organizational systems.

Discussion for Media Use | Prohibit Use of Sanitization-resistant Media (MP-7(2))
Sanitization resistance refers to how resistant media are to non-destructive sanitization techniques with respect to the capability to purge information from media. Certain types of media do not support sanitization commands, or if supported, the interfaces are not supported in a standardized way across these devices. Sanitization-resistant media includes compact flash, embedded flash on boards and devices, solid state drives, and USB removable media.

Media Downgrading (MP-8)

Description for Media Downgrading (MP-8)
a. Establish [Assignment: organization-defined system media downgrading process] that includes employing downgrading mechanisms with strength and integrity commensurate with the security category or classification of the information;
b. Verify that the system media downgrading process is commensurate with the security category and/or classification level of the information to be removed and the access authorizations of the potential recipients of the downgraded information;
c. Identify [Assignment: organization-defined system media requiring downgrading]; and
d. Downgrade the identified system media using the established process.

Discussion for Media Downgrading (MP-8)
Media downgrading applies to digital and non-digital media subject to release outside of the organization, whether the media is considered removable or not. When applied to system media, the downgrading process removes information from the media, typically by security category or classification level, such that the information cannot be retrieved or reconstructed. Downgrading of media includes redacting information to enable wider release and distribution. Downgrading ensures that empty space on the media is devoid of information.

Media Downgrading | Documentation of Process (MP-8(1))

Description for Media Downgrading | Documentation of Process (MP-8(1))
Document system media downgrading actions.

Discussion for Media Downgrading | Documentation of Process (MP-8(1))
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.

Media Downgrading | Equipment Testing (MP-8(2))

Description for Media Downgrading | Equipment Testing (MP-8(2))
Test downgrading equipment and procedures [Assignment: organization-defined frequency] to ensure that downgrading actions are being achieved.

Discussion for Media Downgrading | Equipment Testing (MP-8(2))
None.

Media Downgrading | Controlled Unclassified Information (MP-8(3))

Description for Media Downgrading | Controlled Unclassified Information (MP-8(3))
Downgrade system media containing controlled unclassified information prior to public release.

Discussion for Media Downgrading | Controlled Unclassified Information (MP-8(3))
The downgrading of controlled unclassified information uses approved sanitization tools, techniques, and procedures.

Media Downgrading | Classified Information (MP-8(4))

Description for Media Downgrading | Classified Information (MP-8(4))
Downgrade system media containing classified information prior to release to individuals without required access authorizations.

Discussion for Media Downgrading | Classified Information (MP-8(4))
Downgrading of classified information uses approved sanitization tools, techniques, and procedures to transfer information confirmed to be unclassified from classified systems to unclassified media.

Policy and Procedures (PE-1)

Description for Policy and Procedures (PE-1)
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) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the physical and environmental protection policy and the associated physical and environmental protection controls;
b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures; and
c. Review and update the current physical and environmental protection:
1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

Discussion for Policy and Procedures (PE-1)
Physical and environmental protection policy and procedures address the controls in the PE family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of physical and environmental protection policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, 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. Events that may precipitate an update to physical and environmental protection policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Physical Access Authorizations (PE-2)

Description for Physical Access Authorizations (PE-2)
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 access list detailing authorized facility access by individuals [Assignment: organization-defined frequency]; and
d. Remove individuals from the facility access list when access is no longer required.

Discussion for Physical Access Authorizations (PE-2)
Physical access authorizations apply to employees and visitors. Individuals with permanent physical access authorization credentials are not considered visitors. Authorization credentials include ID badges, identification cards, and smart cards. Organizations determine the strength of authorization credentials needed consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Physical access authorizations may not be necessary to access certain areas within facilities that are designated as publicly accessible.

Physical Access Authorizations | Access by Position or Role (PE-2(1))

Description for Physical Access Authorizations | Access by Position or Role (PE-2(1))
Authorize physical access to the facility where the system resides based on position or role.

Discussion for Physical Access Authorizations | Access by Position or Role (PE-2(1))
Role-based facility access includes access by authorized permanent and regular/routine maintenance personnel, duty officers, and emergency medical staff.

Physical Access Authorizations | Two Forms of Identification (PE-2(2))

Description for Physical Access Authorizations | Two Forms of Identification (PE-2(2))
Require two forms of identification from the following forms of identification for visitor access to the facility where the system resides: [Assignment: organization-defined list of acceptable forms of identification].

Discussion for Physical Access Authorizations | Two Forms of Identification (PE-2(2))
Acceptable forms of identification include passports, REAL ID-compliant drivers' licenses, and Personal Identity Verification (PIV) cards. For gaining access to facilities using automated mechanisms, organizations may use PIV cards, key cards, PINs, and biometrics.

Physical Access Authorizations | Restrict Unescorted Access (PE-2(3))

Description for Physical Access Authorizations | Restrict Unescorted Access (PE-2(3))
Restrict unescorted access to the facility where the system resides to personnel with [Selection (one or more): security clearances for all information contained within the system; formal access authorizations for all information contained within the system; need for access to all information contained within the system; [Assignment: organization-defined physical access authorizations]].

Discussion for Physical Access Authorizations | Restrict Unescorted Access (PE-2(3))
Individuals without required security clearances, access approvals, or need to know are escorted by individuals with appropriate physical access authorizations to ensure that information is not exposed or otherwise compromised.

Physical Access Control (PE-3)

Description for Physical Access Control (PE-3)
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 ingress and egress to the facility using [Selection (one or more): [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 physical access controls];
d. Escort visitors and control visitor activity [Assignment: organization-defined circumstances requiring visitor escorts and control of visitor activity];
e. Secure keys, combinations, and other physical access devices;
f. Inventory [Assignment: organization-defined physical access devices] every [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.

Discussion for Physical Access Control (PE-3)
Physical access control applies to employees and visitors. Individuals with permanent physical access authorizations are not considered visitors. Physical access controls for publicly accessible areas may include physical access control logs/records, guards, or physical access devices and barriers to prevent movement from publicly accessible areas to non-public areas. Organizations determine the types of guards needed, including professional security staff, system users, or administrative staff. Physical access devices include keys, locks, combinations, biometric readers, and card readers. Physical access control systems comply with applicable laws, executive orders, directives, policies, regulations, standards, and guidelines. Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural, automated, or some combination thereof. Physical access points can include facility access points, interior access points to systems that require supplemental access controls, or both. Components of systems may be in areas designated as publicly accessible with organizations controlling access to the components.

Physical Access Control | System Access (PE-3(1))

Description for Physical Access Control | System Access (PE-3(1))
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].

Discussion for Physical Access Control | System Access (PE-3(1))
Control of physical access to the system provides additional physical security for those areas within facilities where there is a concentration of system components.

Physical Access Control | Facility and Systems (PE-3(2))

Description for Physical Access Control | Facility and Systems (PE-3(2))
Perform security checks [Assignment: organization-defined frequency] at the physical perimeter of the facility or system for exfiltration of information or removal of system components.

Discussion for Physical Access Control | Facility and Systems (PE-3(2))
Organizations determine the extent, frequency, and/or randomness of security checks to adequately mitigate risk associated with exfiltration.

Physical Access Control | Continuous Guards (PE-3(3))

Description for Physical Access Control | Continuous Guards (PE-3(3))
Employ guards to control [Assignment: organization-defined physical access points] to the facility where the system resides 24 hours per day, 7 days per week.

Discussion for Physical Access Control | Continuous Guards (PE-3(3))
Employing guards at selected physical access points to the facility provides a more rapid response capability for organizations. Guards also provide the opportunity for human surveillance in areas of the facility not covered by video surveillance.

Physical Access Control | Lockable Casings (PE-3(4))

Description for Physical Access Control | Lockable Casings (PE-3(4))
Use lockable physical casings to protect [Assignment: organization-defined system components] from unauthorized physical access.

Discussion for Physical Access Control | Lockable Casings (PE-3(4))
The greatest risk from the use of portable devices—such as smart phones, tablets, and notebook computers—is theft. Organizations can employ lockable, physical casings to reduce or eliminate the risk of equipment theft. Such casings come in a variety of sizes, from units that protect a single notebook computer to full cabinets that can protect multiple servers, computers, and peripherals. Lockable physical casings can be used in conjunction with cable locks or lockdown plates to prevent the theft of the locked casing containing the computer equipment.

Physical Access Control | Tamper Protection (PE-3(5))

Description for Physical Access Control | Tamper Protection (PE-3(5))
Employ [Assignment: organization-defined anti-tamper technologies] to [Selection (one or more): detect; prevent] physical tampering or alteration of [Assignment: organization-defined hardware components] within the system.

Discussion for Physical Access Control | Tamper Protection (PE-3(5))
Organizations can implement tamper detection and prevention at selected hardware components or implement tamper detection at some components and tamper prevention at other components. Detection and prevention activities can employ many types of anti-tamper technologies, including tamper-detection seals and anti-tamper coatings. Anti-tamper programs help to detect hardware alterations through counterfeiting and other supply chain-related risks.

Emergency Shutoff | Accidental and Unauthorized Activation (PE-10(1))

Description for Emergency Shutoff | Accidental and Unauthorized Activation (PE-10(1))
[Withdrawn: Incorporated into PE-10.]

Discussion for Emergency Shutoff | Accidental and Unauthorized Activation (PE-10(1))

Physical Access Control | Physical Barriers (PE-3(7))

Description for Physical Access Control | Physical Barriers (PE-3(7))
Limit access using physical barriers.

Discussion for Physical Access Control | Physical Barriers (PE-3(7))
Physical barriers include bollards, concrete slabs, jersey walls, and hydraulic active vehicle barriers.

Physical Access Control | Access Control Vestibules (PE-3(8))

Description for Physical Access Control | Access Control Vestibules (PE-3(8))
Employ access control vestibules at [Assignment: organization-defined locations within the facility].

Discussion for Physical Access Control | Access Control Vestibules (PE-3(8))
An access control vestibule is part of a physical access control system that typically provides a space between two sets of interlocking doors. 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. Interlocking door controllers can be used to limit the number of individuals who enter controlled access points and to provide containment areas while authorization for physical access is verified. Interlocking door controllers can be fully automated (i.e., controlling the opening and closing of the doors) or partially automated (i.e., using security guards to control the number of individuals entering the containment area).

Access Control for Transmission (PE-4)

Description for Access Control for Transmission (PE-4)
Control physical access to [Assignment: organization-defined system distribution and transmission lines] within organizational facilities using [Assignment: organization-defined security controls].

Discussion for Access Control for Transmission (PE-4)
Security controls applied to system distribution and transmission lines prevent accidental damage, disruption, and physical tampering. Such controls may also be necessary to prevent eavesdropping or modification of unencrypted transmissions. Security controls used to control physical access to system distribution and transmission lines include disconnected or locked spare jacks, locked wiring closets, protection of cabling by conduit or cable trays, and wiretapping sensors.

Access Control for Output Devices (PE-5)

Description for Access Control for Output Devices (PE-5)
Control physical access to output from [Assignment: organization-defined output devices] to prevent unauthorized individuals from obtaining the output.

Discussion for Access Control for Output Devices (PE-5)
Controlling physical access to output devices includes placing output devices in locked rooms or other secured areas with keypad or card reader access controls and allowing access to authorized individuals only, placing output devices in locations that can be monitored by personnel, installing monitor or screen filters, and using headphones. Examples of output devices include monitors, printers, scanners, audio devices, facsimile machines, and copiers.

Fire Protection | Automatic Fire Suppression (PE-13(3))

Description for Fire Protection | Automatic Fire Suppression (PE-13(3))
[Withdrawn: Incorporated into PE-13(2).]

Discussion for Fire Protection | Automatic Fire Suppression (PE-13(3))

Access Control for Output Devices | Link to Individual Identity (PE-5(2))

Description for Access Control for Output Devices | Link to Individual Identity (PE-5(2))
Link individual identity to receipt of output from output devices.

Discussion for Access Control for Output Devices | Link to Individual Identity (PE-5(2))
Methods for linking individual identity to the receipt of output from output devices include installing security functionality on facsimile machines, copiers, and printers. Such functionality allows organizations to implement authentication on output devices prior to the release of output to individuals.

Location of System Components | Facility Site (PE-18(1))

Description for Location of System Components | Facility Site (PE-18(1))
[Withdrawn: Moved to PE-23.]

Discussion for Location of System Components | Facility Site (PE-18(1))

Monitoring Physical Access (PE-6)

Description for Monitoring Physical Access (PE-6)
a. Monitor physical access to the facility where the system resides to detect and respond 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.

Discussion for Monitoring Physical Access (PE-6)
Physical access monitoring includes publicly accessible areas within organizational facilities. Examples of physical access monitoring include the employment of guards, video surveillance equipment (i.e., cameras), and sensor devices. Reviewing physical access logs can help identify suspicious activity, anomalous events, or potential threats. The reviews can be supported by audit logging controls, such as AU-2, if the access logs are part of an automated system. Organizational incident response capabilities include investigations of physical security incidents and responses to the incidents. Incidents include security violations or suspicious physical access activities. Suspicious physical access activities include accesses outside of normal work hours, repeated accesses to areas not normally accessed, accesses for unusual lengths of time, and out-of-sequence accesses.

Monitoring Physical Access | Intrusion Alarms and Surveillance Equipment (PE-6(1))

Description for Monitoring Physical Access | Intrusion Alarms and Surveillance Equipment (PE-6(1))
Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment.

Discussion for Monitoring Physical Access | Intrusion Alarms and Surveillance Equipment (PE-6(1))
Physical intrusion alarms can be employed to alert security personnel when unauthorized access to the facility is attempted. Alarm systems work in conjunction with physical barriers, physical access control systems, and security guards by triggering a response when these other forms of security have been compromised or breached. Physical intrusion alarms can include different types of sensor devices, such as motion sensors, contact sensors, and broken glass sensors. Surveillance equipment includes video cameras installed at strategic locations throughout the facility.

Monitoring Physical Access | Automated Intrusion Recognition and Responses (PE-6(2))

Description for Monitoring Physical Access | Automated Intrusion Recognition and Responses (PE-6(2))
Recognize [Assignment: organization-defined classes or types of intrusions] and initiate [Assignment: organization-defined response actions] using [Assignment: organization-defined automated mechanisms].

Discussion for Monitoring Physical Access | Automated Intrusion Recognition and Responses (PE-6(2))
Response actions can include notifying selected organizational personnel or law enforcement personnel. Automated mechanisms implemented to initiate response actions include system alert notifications, email and text messages, and activating door locking mechanisms. Physical access monitoring can be coordinated with intrusion detection systems and system monitoring capabilities to provide integrated threat coverage for the organization.

Monitoring Physical Access | Video Surveillance (PE-6(3))

Description for Monitoring Physical Access | Video Surveillance (PE-6(3))
(a) Employ video surveillance of [Assignment: organization-defined operational areas];
(b) Review video recordings [Assignment: organization-defined frequency]; and
(c) Retain video recordings for [Assignment: organization-defined time period].

Discussion for Monitoring Physical Access | Video Surveillance (PE-6(3))
Video surveillance focuses on recording activity in specified areas for the purposes of subsequent review, if circumstances so warrant. Video recordings are typically reviewed to detect anomalous events or incidents. Monitoring the surveillance video is not required, although organizations may choose to do so. There may be legal considerations when performing and retaining video surveillance, especially if such surveillance is in a public location.

Monitoring Physical Access | Monitoring Physical Access to Systems (PE-6(4))

Description for Monitoring Physical Access | Monitoring Physical Access to Systems (PE-6(4))
Monitor physical access to the system in addition to the physical access monitoring of the facility at [Assignment: organization-defined physical spaces containing one or more components of the system].

Discussion for Monitoring Physical Access | Monitoring Physical Access to Systems (PE-6(4))
Monitoring physical access to systems provides additional monitoring for those areas within facilities where there is a concentration of system components, including server rooms, media storage areas, and communications centers. Physical access monitoring can be coordinated with intrusion detection systems and system monitoring capabilities to provide comprehensive and integrated threat coverage for the organization.

Physical Access Control | Facility Penetration Testing (PE-3(6))

Description for Physical Access Control | Facility Penetration Testing (PE-3(6))
[Withdrawn: Incorporated into CA-8.]

Discussion for Physical Access Control | Facility Penetration Testing (PE-3(6))

Visitor Access Records (PE-8)

Description for Visitor Access Records (PE-8)
a. Maintain visitor access records to the facility where the system resides for [Assignment: organization-defined time period];
b. Review visitor access records [Assignment: organization-defined frequency]; and
c. Report anomalies in visitor access records to [Assignment: organization-defined personnel].

Discussion for Visitor Access Records (PE-8)
Visitor access records include the names and organizations of individuals visiting, visitor signatures, forms of identification, dates of access, entry and departure times, purpose of visits, and the names and organizations of individuals visited. Access record reviews determine if access authorizations are current and are still required to support organizational mission and business functions. Access records are not required for publicly accessible areas.

Visitor Access Records | Automated Records Maintenance and Review (PE-8(1))

Description for Visitor Access Records | Automated Records Maintenance and Review (PE-8(1))
Maintain and review visitor access records using [Assignment: organization-defined automated mechanisms].

Discussion for Visitor Access Records | Automated Records Maintenance and Review (PE-8(1))
Visitor access records may be stored and maintained in a database management system that is accessible by organizational personnel. Automated access to such records facilitates record reviews on a regular basis to determine if access authorizations are current and still required to support organizational mission and business functions.

Access Control for Output Devices | Access to Output by Authorized Individuals (PE-5(1))

Description for Access Control for Output Devices | Access to Output by Authorized Individuals (PE-5(1))
[Withdrawn: Incorporated into PE-5.]

Discussion for Access Control for Output Devices | Access to Output by Authorized Individuals (PE-5(1))

Visitor Access Records | Limit Personally Identifiable Information Elements (PE-8(3))

Description for Visitor Access Records | Limit Personally Identifiable Information Elements (PE-8(3))
Limit personally identifiable information contained in visitor access records to the following elements identified in the privacy risk assessment: [Assignment: organization-defined elements].

Discussion for Visitor Access Records | Limit Personally Identifiable Information Elements (PE-8(3))
Organizations may have requirements that specify the contents of visitor access records. Limiting personally identifiable information in visitor access records when such information is not needed for operational purposes helps reduce the level of privacy risk created by a system.

Power Equipment and Cabling (PE-9)

Description for Power Equipment and Cabling (PE-9)
Protect power equipment and power cabling for the system from damage and destruction.

Discussion for Power Equipment and Cabling (PE-9)
Organizations determine the types of protection necessary for the power equipment and cabling employed at different locations that are both internal and external to organizational facilities and environments of operation. Types of power equipment and cabling include internal cabling and uninterruptable power sources in offices or data centers, generators and power cabling outside of buildings, and power sources for self-contained components such as satellites, vehicles, and other deployable systems.

Power Equipment and Cabling | Redundant Cabling (PE-9(1))

Description for Power Equipment and Cabling | Redundant Cabling (PE-9(1))
Employ redundant power cabling paths that are physically separated by [Assignment: organization-defined distance].

Discussion for Power Equipment and Cabling | Redundant Cabling (PE-9(1))
Physically separate and redundant power cables ensure that power continues to flow in the event that one of the cables is cut or otherwise damaged.

Power Equipment and Cabling | Automatic Voltage Controls (PE-9(2))

Description for Power Equipment and Cabling | Automatic Voltage Controls (PE-9(2))
Employ automatic voltage controls for [Assignment: organization-defined critical system components].

Discussion for Power Equipment and Cabling | Automatic Voltage Controls (PE-9(2))
Automatic voltage controls can monitor and control voltage. Such controls include voltage regulators, voltage conditioners, and voltage stabilizers.

Emergency Shutoff (PE-10)

Description for Emergency Shutoff (PE-10)
a. Provide the capability of shutting off power to [Assignment: organization-defined system or individual system components] in emergency situations;
b. Place emergency shutoff switches or devices in [Assignment: organization-defined location by system or system component] to facilitate access for authorized personnel; and
c. Protect emergency power shutoff capability from unauthorized activation.

Discussion for Emergency Shutoff (PE-10)
Emergency power shutoff primarily applies to organizational facilities that contain concentrations of system resources, including data centers, mainframe computer rooms, server rooms, and areas with computer-controlled machinery.

Access Control for Output Devices | Marking Output Devices (PE-5(3))

Description for Access Control for Output Devices | Marking Output Devices (PE-5(3))
[Withdrawn: Incorporated into PE-22.]

Discussion for Access Control for Output Devices | Marking Output Devices (PE-5(3))

Emergency Power (PE-11)

Description for Emergency Power (PE-11)
Provide an uninterruptible power supply to facilitate [Selection (one or more): an orderly shutdown of the system; transition of the system to long-term alternate power] in the event of a primary power source loss.

Discussion for Emergency Power (PE-11)
An uninterruptible power supply (UPS) is an electrical system or mechanism that provides emergency power when there is a failure of the main power source. A UPS is typically used to protect computers, data centers, telecommunication equipment, or other electrical equipment where an unexpected power disruption could cause injuries, fatalities, serious mission or business disruption, or loss of data or information. A UPS differs from an emergency power system or backup generator in that the UPS provides near-instantaneous protection from unanticipated power interruptions from the main power source by providing energy stored in batteries, supercapacitors, or flywheels. The battery duration of a UPS is relatively short but provides sufficient time to start a standby power source, such as a backup generator, or properly shut down the system.

Emergency Power | Alternate Power Supply — Minimal Operational Capability (PE-11(1))

Description for Emergency Power | Alternate Power Supply — Minimal Operational Capability (PE-11(1))
Provide an alternate power supply for the system that is activated [Selection: manually; automatically] and that can maintain minimally required operational capability in the event of an extended loss of the primary power source.

Discussion for Emergency Power | Alternate Power Supply — Minimal Operational Capability (PE-11(1))
Provision of an alternate power supply with minimal operating capability can be satisfied by accessing a secondary commercial power supply or other external power supply.

Emergency Power | Alternate Power Supply — Self-contained (PE-11(2))

Description for Emergency Power | Alternate Power Supply — Self-contained (PE-11(2))
Provide an alternate power supply for the system that is activated [Selection: manually; automatically] and that is:
(a) Self-contained;
(b) Not reliant on external power generation; and
(c) Capable of maintaining [Selection: minimally required operational capability; full operational capability] in the event of an extended loss of the primary power source.

Discussion for Emergency Power | Alternate Power Supply — Self-contained (PE-11(2))
The provision of a long-term, self-contained power supply can be satisfied by using one or more generators with sufficient capacity to meet the needs of the organization.

Emergency Lighting (PE-12)

Description for Emergency Lighting (PE-12)
Employ and maintain automatic emergency lighting for the system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

Discussion for Emergency Lighting (PE-12)
The provision of emergency lighting applies primarily to organizational facilities that contain concentrations of system resources, including data centers, server rooms, and mainframe computer rooms. Emergency lighting provisions for the system are described in the contingency plan for the organization. If emergency lighting for the system fails or cannot be provided, organizations consider alternate processing sites for power-related contingencies.

Emergency Lighting | Essential Mission and Business Functions (PE-12(1))

Description for Emergency Lighting | Essential Mission and Business Functions (PE-12(1))
Provide emergency lighting for all areas within the facility supporting essential mission and business functions.

Discussion for Emergency Lighting | Essential Mission and Business Functions (PE-12(1))
Organizations define their essential missions and functions.

Fire Protection (PE-13)

Description for Fire Protection (PE-13)
Employ and maintain fire detection and suppression systems that are supported by an independent energy source.

Discussion for Fire Protection (PE-13)
The provision of fire detection and suppression systems applies primarily to organizational facilities that contain 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 and smoke detectors. An independent energy source is an energy source, such as a microgrid, that is separate, or can be separated, from the energy sources providing power for the other parts of the facility.

Fire Protection | Detection Systems — Automatic Activation and Notification (PE-13(1))

Description for Fire Protection | Detection Systems — Automatic Activation and Notification (PE-13(1))
Employ fire detection systems that activate automatically and notify [Assignment: organization-defined personnel or roles] and [Assignment: organization-defined emergency responders] in the event of a fire.

Discussion for Fire Protection | Detection Systems — Automatic Activation and Notification (PE-13(1))
Organizations can identify personnel, roles, and emergency responders if individuals on the notification list need to have access authorizations or clearances (e.g., to enter to facilities where access is restricted due to the classification or impact level of information within the facility). Notification mechanisms may require independent energy sources to ensure that the notification capability is not adversely affected by the fire.

Fire Protection | Suppression Systems — Automatic Activation and Notification (PE-13(2))

Description for Fire Protection | Suppression Systems — Automatic Activation and Notification (PE-13(2))
(a) Employ fire suppression systems that activate automatically and notify [Assignment: organization-defined personnel or roles] and [Assignment: organization-defined emergency responders]; and
(b) Employ an automatic fire suppression capability when the facility is not staffed on a continuous basis.

Discussion for Fire Protection | Suppression Systems — Automatic Activation and Notification (PE-13(2))
Organizations can identify specific personnel, roles, and emergency responders if individuals on the notification list need to have appropriate access authorizations and/or clearances (e.g., to enter to facilities where access is restricted due to the impact level or classification of information within the facility). Notification mechanisms may require independent energy sources to ensure that the notification capability is not adversely affected by the fire.

Visitor Control (PE-7)

Description for Visitor Control (PE-7)
[Withdrawn: Incorporated into PE-2 and PE-3.]

Discussion for Visitor Control (PE-7)

Fire Protection | Inspections (PE-13(4))

Description for Fire Protection | Inspections (PE-13(4))
Ensure that the facility undergoes [Assignment: organization-defined frequency] fire protection inspections by authorized and qualified inspectors and identified deficiencies are resolved within [Assignment: organization-defined time period].

Discussion for Fire Protection | Inspections (PE-13(4))
Authorized and qualified personnel within the jurisdiction of the organization include state, county, and city fire inspectors and fire marshals. Organizations provide escorts during inspections in situations where the systems that reside within the facilities contain sensitive information.

Environmental Controls (PE-14)

Description for Environmental Controls (PE-14)
a. Maintain [Selection (one or more): temperature; humidity; pressure; radiation; [Assignment: organization-defined environmental control]] levels within the facility where the system resides at [Assignment: organization-defined acceptable levels]; and
b. Monitor environmental control levels [Assignment: organization-defined frequency].

Discussion for Environmental Controls (PE-14)
The provision of environmental controls applies primarily to organizational facilities that contain concentrations of system resources (e.g., data centers, mainframe computer rooms, and server rooms). Insufficient environmental controls, especially in very harsh environments, can have a significant adverse impact on the availability of systems and system components that are needed to support organizational mission and business functions.

Environmental Controls | Automatic Controls (PE-14(1))

Description for Environmental Controls | Automatic Controls (PE-14(1))
Employ the following automatic environmental controls in the facility to prevent fluctuations potentially harmful to the system: [Assignment: organization-defined automatic environmental controls].

Discussion for Environmental Controls | Automatic Controls (PE-14(1))
The implementation of automatic environmental controls provides an immediate response to environmental conditions that can damage, degrade, or destroy organizational systems or systems components.

Environmental Controls | Monitoring with Alarms and Notifications (PE-14(2))

Description for Environmental Controls | Monitoring with Alarms and Notifications (PE-14(2))
Employ environmental control monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment to [Assignment: organization-defined personnel or roles].

Discussion for Environmental Controls | Monitoring with Alarms and Notifications (PE-14(2))
The alarm or notification may be an audible alarm or a visual message in real time to personnel or roles defined by the organization. Such alarms and notifications can help minimize harm to individuals and damage to organizational assets by facilitating a timely incident response.

Water Damage Protection (PE-15)

Description for Water Damage Protection (PE-15)
Protect the system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

Discussion for Water Damage Protection (PE-15)
The provision of water damage protection primarily applies to organizational facilities that contain concentrations of system resources, including data centers, server rooms, and mainframe computer rooms. Isolation valves can be employed in addition to or in lieu of master shutoff valves to shut off water supplies in specific areas of concern without affecting entire organizations.

Water Damage Protection | Automation Support (PE-15(1))

Description for Water Damage Protection | Automation Support (PE-15(1))
Detect the presence of water near the system and alert [Assignment: organization-defined personnel or roles] using [Assignment: organization-defined automated mechanisms].

Discussion for Water Damage Protection | Automation Support (PE-15(1))
Automated mechanisms include notification systems, water detection sensors, and alarms.

Delivery and Removal (PE-16)

Description for Delivery and Removal (PE-16)
a. Authorize and control [Assignment: organization-defined types of system components] entering and exiting the facility; and
b. Maintain records of the system components.

Discussion for Delivery and Removal (PE-16)
Enforcing authorizations for entry and exit of system components may require restricting access to delivery areas and isolating the areas from the system and media libraries.

Alternate Work Site (PE-17)

Description for Alternate Work Site (PE-17)
a. Determine and document the [Assignment: organization-defined alternate work sites] allowed for use by employees;
b. Employ the following controls at alternate work sites: [Assignment: organization-defined controls];
c. Assess the effectiveness of controls at alternate work sites; and
d. Provide a means for employees to communicate with information security and privacy personnel in case of incidents.

Discussion for Alternate Work Site (PE-17)
Alternate work sites include government facilities or the private residences of employees. While distinct from alternative processing sites, alternate work sites can provide readily available alternate locations during contingency operations. Organizations can define different sets of controls for specific alternate work sites or types of sites depending on the work-related activities conducted at the sites. Implementing and assessing the effectiveness of organization-defined controls and

providing a means to communicate incidents at alternate work sites supports the contingency planning activities of organizations.

Location of System Components (PE-18)

Description for Location of System Components (PE-18)
Position system components within the facility to minimize potential damage from [Assignment: organization-defined physical and environmental hazards] and to minimize the opportunity for unauthorized access.

Discussion for Location of System Components (PE-18)
Physical and environmental hazards include floods, fires, tornadoes, earthquakes, hurricanes, terrorism, vandalism, an electromagnetic pulse, electrical interference, and other forms of incoming electromagnetic radiation. Organizations consider the location of entry points where unauthorized individuals, while not being granted access, might nonetheless be near systems. Such proximity can increase the risk of unauthorized access to organizational communications using wireless packet sniffers or microphones, or unauthorized disclosure of information.

Visitor Access Records | Physical Access Records (PE-8(2))

Description for Visitor Access Records | Physical Access Records (PE-8(2))
[Withdrawn: Incorporated into PE-2.]

Discussion for Visitor Access Records | Physical Access Records (PE-8(2))

Information Leakage (PE-19)

Description for Information Leakage (PE-19)
Protect the system from information leakage due to electromagnetic signals emanations.

Discussion for Information Leakage (PE-19)
Information leakage is the intentional or unintentional release of data or information to an untrusted 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.

Information Leakage | National Emissions Policies and Procedures (PE-19(1))

Description for Information Leakage | National Emissions Policies and Procedures (PE-19(1))
Protect system components, associated data communications, and networks in accordance with national Emissions Security policies and procedures based on the security category or classification of the information.

Discussion for Information Leakage | National Emissions Policies and Procedures (PE-19(1))
Emissions Security (EMSEC) policies include the former TEMPEST policies.

Asset Monitoring and Tracking (PE-20)

Description for Asset Monitoring and Tracking (PE-20)
Employ [Assignment: organization-defined asset location technologies] to track and monitor the location and movement of [Assignment: organization-defined assets] within [Assignment: organization-defined controlled areas].

Discussion for Asset Monitoring and Tracking (PE-20)
Asset location technologies can help ensure that critical assets—including vehicles, equipment, and system components—remain in authorized locations.
Organizations consult with the Office of the General Counsel and senior agency official for privacy regarding the deployment and use of asset location technologies to address potential privacy concerns.

Electromagnetic Pulse Protection (PE-21)

Description for Electromagnetic Pulse Protection (PE-21)
Employ [Assignment: organization-defined protective measures] against electromagnetic pulse damage for [Assignment: organization-defined systems and system components].

Discussion for Electromagnetic Pulse Protection (PE-21)
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, ferro-resonant transformers, and earth grounding. EMP protection may be especially significant for systems and applications that are part of the U.S. critical infrastructure.

Component Marking (PE-22)

Description for Component Marking (PE-22)
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.

Discussion for Component Marking (PE-22)
Hardware components that may require marking include input and output devices. Input devices include desktop and notebook computers, keyboards, tablets, and smart phones. Output devices include printers, monitors/video displays, facsimile machines, scanners, copiers, and audio devices. Permissions controlling output to the output devices are addressed in AC-3 or AC-4. Components are marked to indicate the impact level or classification level of the system to which the devices are connected, or the impact level or classification level of the information permitted to be output. Security marking refers to the use of human-readable security attributes. Security labeling refers to the use of security attributes for internal system data structures. Security marking is generally not required for hardware components that process, store, or transmit information determined by organizations to be in the public domain or to be publicly releasable. However, organizations may require markings for hardware components that process, store, or transmit public information in order to indicate that such information is publicly releasable. Marking of system hardware components reflects applicable laws, executive orders, directives, policies, regulations, and standards.

Facility Location (PE-23)

Description for Facility Location (PE-23)
a. Plan the location or site of the facility where the system resides considering physical and environmental hazards; and
b. For existing facilities, consider the physical and environmental hazards in the organizational risk management strategy.

Discussion for Facility Location (PE-23)
Physical and environmental hazards include floods, fires, tornadoes, earthquakes, hurricanes, terrorism, vandalism, an electromagnetic pulse, electrical interference, and other forms of incoming electromagnetic radiation. The location of system components within the facility is addressed in PE-18.

Policy and Procedures (PL-1)

Description for Policy and Procedures (PL-1)
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] planning policy that:
(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the planning policy and the associated planning controls;
b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the planning policy and procedures; and
c. Review and update the current planning:
1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

Discussion for Policy and Procedures (PL-1)
Planning policy and procedures for the controls in the PL family implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to 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 mission level or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission/business processes, 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. Events that may precipitate an update to planning policy and procedures include, but are not limited to, assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

System Security and Privacy Plans (PL-2)

Description for System Security and Privacy Plans (PL-2)
a. Develop security and privacy plans for the system that:
1. Are consistent with the organization's enterprise architecture;
2. Explicitly define the constituent system components;
3. Describe the operational context of the system in terms of mission and business processes;
4. Identify the individuals that fulfill system roles and responsibilities;
5. Identify the information types processed, stored, and transmitted by the system;
6. Provide the security categorization of the system, including supporting rationale;
7. Describe any specific threats to the system that are of concern to the organization;
8. Provide the results of a privacy risk assessment for systems processing personally identifiable information;
9. Describe the operational environment for the system and any dependencies on or connections to other systems or system components;
10. Provide an overview of the security and privacy requirements for the system;
11. Identify any relevant control baselines or overlays, if applicable;
12. Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions;
13. Include risk determinations for security and privacy architecture and design decisions;
14. Include security- and privacy-related activities affecting the system that require planning and coordination with [Assignment: organization-defined individuals or groups]; and
15. Are reviewed and approved by the authorizing official or designated representative prior to plan implementation.
b. Distribute copies of the plans and communicate subsequent changes to the plans to [Assignment: organization-defined personnel or roles];
c. Review the plans [Assignment: organization-defined frequency];
d. Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments; and
e. Protect the plans from unauthorized disclosure and modification.

Discussion for System Security and Privacy Plans (PL-2)
System security and privacy plans are scoped to the system and system components within the defined authorization boundary and contain an overview of the security and privacy requirements for the system and the controls selected to satisfy the requirements. The plans describe the intended application of each selected control in the context of the system with a sufficient level of detail to correctly implement the control and to subsequently assess the effectiveness of the control. The control documentation describes how system-specific and hybrid

controls are implemented and the plans and expectations regarding the functionality of the system. System security and privacy plans can also be used in the design and development of systems in support of life cycle-based security and privacy engineering processes. System security and privacy plans are living documents that are updated and adapted throughout the system development life cycle (e.g., during capability determination, analysis of alternatives, requests for proposal, and design reviews). Section 2.1 describes the different types of requirements that are relevant to organizations during the system development life cycle and the relationship between requirements and controls.

Organizations may develop a single, integrated security and privacy plan or maintain separate plans. Security and privacy plans relate security and privacy requirements to a set of controls and control enhancements. The plans describe how the controls and control enhancements meet the security and privacy requirements but do not provide detailed, technical descriptions of the design or implementation of the controls and control enhancements. Security and privacy plans contain sufficient information (including specifications of control parameter values for selection and assignment operations explicitly or by reference) to enable a design and implementation that is unambiguously compliant with the intent of the plans and subsequent determinations of risk to organizational operations and assets, individuals, other organizations, and the Nation if the plan is implemented.

Security and privacy plans need not be single documents. The plans can be a collection of various documents, including documents that already exist. Effective security and privacy plans make extensive use of references to policies, procedures, and additional documents, including design and implementation specifications where more detailed information can be obtained. The use of references helps reduce the documentation associated with security and privacy programs and maintains the security- and privacy-related information in other established management and operational areas, including enterprise architecture, system development life cycle, systems engineering, and acquisition. Security and privacy plans need not contain detailed contingency plan or incident response plan information but can instead provide—explicitly or by reference—sufficient information to define what needs to be accomplished by those plans.

Security- and privacy-related activities that may require coordination and planning with other individuals or groups within the organization include assessments, audits, inspections, hardware and software maintenance, acquisition and supply chain risk management, patch management, and contingency plan testing. Planning and coordination include emergency and nonemergency (i.e., planned or non-urgent unplanned) situations. The process defined by organizations to plan and coordinate security- and privacy-related activities can also be included in other documents, as appropriate.

System Security and Privacy Plans | Concept of Operations (PL-2(1))

Description for System Security and Privacy Plans | Concept of Operations (PL-2(1))
[Withdrawn: Incorporated into PL-7.]

Discussion for System Security and Privacy Plans | Concept of Operations (PL-2(1))

System Security and Privacy Plans | Functional Architecture (PL-2(2))

Description for System Security and Privacy Plans | Functional Architecture (PL-2(2))
[Withdrawn: Incorporated into PL-8.]

Discussion for System Security and Privacy Plans | Functional Architecture (PL-2(2))

System Security and Privacy Plans | Plan and Coordinate with Other Organizational Entities (PL-2(3))

Description for System Security and Privacy Plans | Plan and Coordinate with Other Organizational Entities (PL-2(3))
[Withdrawn: Incorporated into PL-2.]

Discussion for System Security and Privacy Plans | Plan and Coordinate with Other Organizational Entities (PL-2(3))

System Security Plan Update (PL-3)

Description for System Security Plan Update (PL-3)
[Withdrawn: Incorporated into PL-2.]

Discussion for System Security Plan Update (PL-3)

Rules of Behavior (PL-4)

Description for Rules of Behavior (PL-4)
a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy;
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. Review and update the rules of behavior [Assignment: organization-defined frequency]; and
d. Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge [Selection (one or more): [Assignment: organization-defined frequency]; when the rules are revised or updated].

Discussion for Rules of Behavior (PL-4)
Rules of behavior represent a type of access agreement for organizational users. Other types of access agreements include nondisclosure agreements, conflict-of-interest agreements, and acceptable use agreements (see PS-6). Organizations consider rules of behavior based on individual user roles and responsibilities and differentiate between rules that apply to privileged users and rules that apply to general users. Establishing rules of behavior for some types of non-organizational users, including individuals who receive information from federal systems, is often not feasible given the large number of such users and the limited nature of their interactions with the systems. Rules of behavior for organizational and non-organizational users can also be established in AC-8. The related controls section

provides a list of controls that are relevant to organizational rules of behavior. PL-4b, the documented acknowledgment portion of the control, may be satisfied by the literacy training and awareness and role-based training programs conducted by organizations if such training includes rules of behavior. Documented acknowledgements for rules of behavior include electronic or physical signatures and electronic agreement check boxes or radio buttons.

Rules of Behavior | Social Media and External Site/application Usage Restrictions (PL-4(1))

Description for Rules of Behavior | Social Media and External Site/application Usage Restrictions (PL-4(1))
Include in the rules of behavior, restrictions on:
(a) Use of social media, social networking sites, and external sites/applications;
(b) Posting organizational information on public websites; and
(c) Use of organization-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications.

Discussion for Rules of Behavior | Social Media and External Site/application Usage Restrictions (PL-4(1))
Social media, social networking, and external site/application usage restrictions address rules of behavior related to the use of social media, social networking, and external sites when organizational personnel are using such sites for official duties or in the conduct of official business, when organizational information is involved in social media and social networking transactions, and when personnel access social media and networking sites from organizational systems. Organizations also address specific rules that prevent unauthorized entities from obtaining non-public organizational information from social media and networking sites either directly or through inference. Non-public information includes personally identifiable information and system account information.

Privacy Impact Assessment (PL-5)

Description for Privacy Impact Assessment (PL-5)
[Withdrawn: Incorporated into RA-8.]

Discussion for Privacy Impact Assessment (PL-5)

Security-related Activity Planning (PL-6)

Description for Security-related Activity Planning (PL-6)
[Withdrawn: Incorporated into PL-2.]

Discussion for Security-related Activity Planning (PL-6)

Concept of Operations (PL-7)

Description for Concept of Operations (PL-7)
a. Develop a Concept of Operations (CONOPS) for the system describing how the organization intends to operate the system from the perspective of information security and privacy; and
b. Review and update the CONOPS [Assignment: organization-defined frequency].

Discussion for Concept of Operations (PL-7)
The CONOPS may be included in the security or privacy plans for the system or in other system 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 plans, security and privacy architectures, and other organizational documents, such as procurement specifications, system development life cycle documents, and systems engineering documents.

Security and Privacy Architectures (PL-8)

Description for Security and Privacy Architectures (PL-8)
a. Develop security and privacy architectures for the system that:
1. Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information;
2. Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals;
3. Describe how the architectures are integrated into and support the enterprise architecture; and
4. Describe any assumptions about, and dependencies on, external systems and services;
b. Review and update the architectures [Assignment: organization-defined frequency] to reflect changes in the enterprise architecture; and
c. Reflect planned architecture changes in security and privacy plans, Concept of Operations (CONOPS), criticality analysis, organizational procedures, and procurements and acquisitions.

Discussion for Security and Privacy Architectures (PL-8)
The security and privacy architectures at the system level are consistent with the organization-wide security and privacy architectures described in PM-7, which are integral to and developed as part of the enterprise architecture. The architectures include an architectural description, the allocation of security and privacy functionality (including controls), security- and privacy-related information for external interfaces, information being exchanged across the interfaces, and the protection mechanisms associated with each interface. The architectures can also include other information, such as user roles and the access privileges assigned to each role; security and privacy requirements; types of information processed, stored, and transmitted by the system; supply chain risk management requirements; restoration priorities of information and system services; and other protection needs.
SP 800-160-1 provides guidance on the use of security architectures as part of the system development life cycle process. OMB M-19-03 requires the use of the systems security engineering concepts described in SP 800-160-1 for high value assets. Security and privacy architectures are reviewed and updated throughout the system development life cycle, from analysis of alternatives through review of the proposed architecture in the RFP responses to the design reviews before and during implementation (e.g., during preliminary design reviews and critical design reviews).
In today's modern computing architectures, it is becoming less common for organizations to control all information resources. There may be key dependencies on external information services and service providers. Describing such dependencies in the security and privacy architectures is necessary for developing a comprehensive mission and business protection strategy. Establishing,

developing, documenting, and maintaining under configuration control a baseline configuration for organizational systems is critical to implementing and maintaining effective architectures. The development of the architectures is coordinated with the senior agency information security officer and the senior agency official for privacy to ensure that the controls needed to support security and privacy requirements are identified and effectively implemented. In many circumstances, there may be no distinction between the security and privacy architecture for a system. In other circumstances, security objectives may be adequately satisfied, but privacy objectives may only be partially satisfied by the security requirements. In these cases, consideration of the privacy requirements needed to achieve satisfaction will result in a distinct privacy architecture. The documentation, however, may simply reflect the combined architectures.

PL-8 is primarily directed at organizations to ensure that architectures are developed for the system and, moreover, that the architectures are integrated with or tightly coupled to the enterprise architecture. In contrast, SA-17 is primarily directed at the external information technology product and system developers and integrators. SA-17, which is complementary to PL-8, is selected when organizations outsource the development of systems or components to external entities and when there is a need to demonstrate consistency with the organization's enterprise architecture and security and privacy architectures.

Security and Privacy Architectures | Defense in Depth (PL-8(1))

Description for Security and Privacy Architectures | Defense in Depth (PL-8(1))
Design the security and privacy architectures for the system using a defense-in-depth approach that:
(a) Allocates [Assignment: organization-defined controls] to [Assignment: organization-defined locations and architectural layers]; and
(b) Ensures that the allocated controls operate in a coordinated and mutually reinforcing manner.

Discussion for Security and Privacy Architectures | Defense in Depth (PL-8(1))
Organizations strategically allocate security and privacy controls in the security and privacy architectures so that adversaries must overcome multiple controls to achieve their objective. Requiring adversaries to defeat multiple controls makes it more difficult to attack information resources by increasing the work factor of the adversary; it also increases the likelihood of detection. The coordination of allocated controls is essential to ensure that an attack that involves one control does not create adverse, unintended consequences by interfering with other controls. Unintended consequences can include system lockout and cascading alarms. The placement of controls in systems and organizations is an important activity that requires thoughtful analysis. The value of organizational assets is an important consideration in providing additional layering. Defense-in-depth architectural approaches include modularity and layering (see SA-8(3)), separation of system and user functionality (see SC-2), and security function isolation (see SC-3).

Security and Privacy Architectures | Supplier Diversity (PL-8(2))

Description for Security and Privacy Architectures | Supplier Diversity (PL-8(2))
Require that [Assignment: organization-defined controls] allocated to [Assignment: organization-defined locations and architectural layers] are obtained from different suppliers.

Discussion for Security and Privacy Architectures | Supplier Diversity (PL-8(2))
Information technology products have different strengths and weaknesses. Providing a broad spectrum of products complements the individual offerings. For example, vendors offering malicious code protection typically update their products at different times, often developing solutions for known viruses, Trojans, or worms based on their priorities and development schedules. By deploying different products at different locations, there is an increased likelihood that at least one of the products will detect the malicious code. With respect to privacy, vendors may offer products that track personally identifiable information in systems. Products may use different tracking methods. Using multiple products may result in more assurance that personally identifiable information is inventoried.

Central Management (PL-9)

Description for Central Management (PL-9)
Centrally manage [Assignment: organization-defined controls and related processes].

Discussion for Central Management (PL-9)
Central management refers to organization-wide management and implementation of selected controls and processes. This includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed controls and processes. As the central management of controls is generally associated with the concept of common (inherited) controls, such management promotes and facilitates standardization of control implementations and management and the judicious use of organizational resources. Centrally managed controls and processes may also meet independence requirements for assessments in support of initial and ongoing authorizations to operate and as part of organizational continuous monitoring.
Automated tools (e.g., security information and event management tools or enterprise security monitoring and management tools) can improve the accuracy, consistency, and availability of information associated with centrally managed controls and processes. Automation can also provide data aggregation and data correlation capabilities; alerting mechanisms; and dashboards to support risk-based decision-making within the organization.
As part of the control selection processes, organizations determine the controls that may be suitable for central management based on resources and capabilities. It is not always possible to centrally manage every aspect of a control. In such cases, the control can be treated as a hybrid control with the control managed and implemented centrally or at the system level. The controls and control enhancements that are candidates for full or partial central management include but are not limited to: AC-2(1), AC-2(2), AC-2(3), AC-2(4), AC-4(all), AC-17(1), AC-17(2), AC-17(3), AC-17(9), AC-18(1), AC-18(3), AC-18(4), AC-18(5), AC-19(4), AC-22, AC-23, AT-2(1), AT-2(2), AT-3(1), AT-3(2), AT-3(3), AT-4, AU-3, AU-6(1), AU-6(3), AU-6(5), AU-6(6), AU-6(9), AU-7(1), AU-7(2), AU-11, AU-13, AU-16, CA-2(1), CA-2(2), CA-2(3), CA-3(1), CA-3(2), CA-3(3), CA-7(1), CA-9, CM-2(2), CM-3(1), CM-3(4), CM-4, CM-6, CM-6(1), CM-7(2), CM-7(4), CM-7(5), CM-8(all), CM-9(1), CM-10, CM-11, CP-7(all), CP-8(all), SC-43, SI-2, SI-3, SI-4(all), SI-7, SI-8.

Baseline Selection (PL-10)

Description for Baseline Selection (PL-10)
Select a control baseline for the system.

Discussion for Baseline Selection (PL-10)
Control baselines are predefined sets of controls specifically assembled to address the protection needs of a group, organization, or community of interest. Controls are chosen for baselines to either satisfy mandates imposed by laws, executive orders, directives, regulations, policies, standards, and guidelines or 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 individuals' privacy, information, and information systems with subsequent tailoring actions to manage risk in accordance with mission, business, or other constraints (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 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. CNSSI 1253 provides guidance on control baselines for national security systems.

Baseline Tailoring (PL-11)

Description for Baseline Tailoring (PL-11)
Tailor the selected control baseline by applying specified tailoring actions.

Discussion for Baseline Tailoring (PL-11)
The concept of tailoring allows organizations to specialize or customize a set of baseline controls by applying a defined set of tailoring actions. Tailoring actions facilitate such specialization and customization by allowing organizations to develop security and privacy plans that reflect their specific mission and business functions, the environments where their systems operate, the threats and vulnerabilities that can affect their systems, and any other conditions or situations that can impact their mission or business success. Tailoring guidance is provided in SP 800-53B. Tailoring a control baseline is accomplished by identifying and designating common controls, applying scoping considerations, selecting compensating controls, assigning values to control parameters, supplementing the control baseline with additional controls as needed, and providing information for control implementation. The general tailoring actions in SP 800-53B can be supplemented with additional actions based on the needs of organizations. Tailoring actions can be applied to the baselines in SP 800-53B in accordance with the security and privacy requirements from FISMA, PRIVACT, and OMB A-130. Alternatively, other communities of interest adopting different control baselines can apply the tailoring actions in SP 800-53B to specialize or customize the controls that represent the specific needs and concerns of those entities.

Information Security Program Plan (PM-1)

Description for Information Security Program Plan (PM-1)
a. Develop and disseminate an organization-wide information security program plan that:
1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;
2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
3. Reflects the coordination among organizational entities responsible for information security; and
4. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation;
b. Review and update the organization-wide information security program plan [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
c. Protect the information security program plan from unauthorized disclosure and modification.

Discussion for Information Security Program Plan (PM-1)
An information security program plan is a formal document that provides an overview of the security requirements for an organization-wide information security program and describes the program management controls and common controls in place or planned for meeting those requirements. An information security program plan can be represented in a single document or compilations of documents. Privacy program plans and supply chain risk management plans are addressed separately in PM-18 and SR-2, respectively.
An information security program plan documents implementation details about program management and common controls. The plan provides sufficient information about the controls (including specification of parameters for assignment and selection operations, explicitly or by reference) to enable implementations that are unambiguously compliant with the intent of the plan and a determination of the risk to be incurred if the plan is implemented as intended. Updates to information security program plans include organizational changes and problems identified during plan implementation or control assessments.
Program management controls may be implemented at the organization level or the mission or business process level, and are essential for managing the organization's information security program. Program management controls are distinct from common, system-specific, and hybrid controls because program

management controls are independent of any particular system. Together, the individual system security plans and the organization-wide information security program plan provide complete coverage for the security controls employed within the organization.

Common controls available for inheritance by organizational systems are documented in an appendix to the organization's information security program plan unless the controls are included in a separate security plan for a system. The organization-wide information security program plan indicates which separate security plans contain descriptions of common controls.

Events that may precipitate an update to the information security program plan include, but are not limited to, organization-wide assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines.

Information Security Program Leadership Role (PM-2)

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

Discussion for Information Security Program Leadership Role (PM-2)
The senior agency information security officer is an organizational official. For federal agencies (as defined by applicable laws, executive orders, regulations, directives, policies, and standards), this official is the senior agency information security officer. Organizations may also refer to this official as the senior information security officer or chief information security officer.

Information Security and Privacy Resources (PM-3)

Description for Information Security and Privacy Resources (PM-3)
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
c. Make available for expenditure, the planned information security and privacy resources.

Discussion for Information Security and Privacy Resources (PM-3)
Organizations consider establishing champions for information security and privacy and, as part of including the necessary resources, assign specialized expertise and resources as needed. Organizations may designate and empower an Investment Review Board or similar group to manage and provide oversight for the information security and privacy aspects of the capital planning and investment control process.

Plan of Action and Milestones Process (PM-4)

Description for Plan of Action and Milestones Process (PM-4)
a. Implement a process to ensure that plans of action and milestones for the information security, privacy, and supply chain risk management programs and associated organizational systems:
1. Are developed and maintained;
2. Document the remedial information security, privacy, and supply chain risk management actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and
3. 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.

Discussion for Plan of Action and Milestones Process (PM-4)
The plan of action and milestones is a key organizational document and is subject to reporting requirements established by the Office of Management and Budget. Organizations develop plans of action and milestones with an organization-wide perspective, prioritizing risk response actions and ensuring consistency with the goals and objectives of the organization. Plan of action and milestones updates are based on findings from control assessments and continuous monitoring activities. There can be multiple plans of action and milestones corresponding to the

information system level, mission/business process level, and organizational/governance level. While plans of action and milestones are required for federal organizations, other types of organizations can help reduce risk by documenting and tracking planned remediations. Specific guidance on plans of action and milestones at the system level is provided in CA-5.

System Inventory (PM-5)

Description for System Inventory (PM-5)
Develop and update [Assignment: organization-defined frequency] an inventory of organizational systems.

Discussion for System Inventory (PM-5)
OMB A-130 provides guidance on developing systems inventories and associated reporting requirements. System inventory refers to an organization-wide inventory of systems, not system components as described in CM-8.

System Inventory | Inventory of Personally Identifiable Information (PM-5(1))

Description for System Inventory | Inventory of Personally Identifiable Information (PM-5(1))
Establish, maintain, and update [Assignment: organization-defined frequency] an inventory of all systems, applications, and projects that process personally identifiable information.

Discussion for System Inventory | Inventory of Personally Identifiable Information (PM-5(1))
An inventory of systems, applications, and projects that process personally identifiable information supports the mapping of data actions, providing individuals with privacy notices, maintaining accurate personally identifiable information, and limiting the processing of personally identifiable information when such information is not needed for operational purposes. Organizations may use this inventory to ensure that systems only process the personally identifiable information for authorized purposes and that this processing is still relevant and necessary for the purpose specified therein.

Measures of Performance (PM-6)

Description for Measures of Performance (PM-6)
Develop, monitor, and report on the results of information security and privacy measures of performance.

Discussion for Measures of Performance (PM-6)
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. To facilitate security and privacy risk management, organizations consider aligning measures of performance with the organizational risk tolerance as defined in the risk management strategy.

Enterprise Architecture (PM-7)

Description for Enterprise Architecture (PM-7)
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.

Discussion for Enterprise Architecture (PM-7)
The integration of security and privacy requirements and controls into the enterprise architecture helps to ensure that security and privacy considerations are addressed throughout the system development life cycle and are explicitly related to the organization's mission and business processes. The process of security and privacy requirements integration also embeds into the enterprise architecture and 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 PL-8, the security and privacy architectures are developed at a level that represents 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.

Enterprise Architecture | Offloading (PM-7(1))

Description for Enterprise Architecture | Offloading (PM-7(1))
Offload [Assignment: organization-defined non-essential functions or services] to other systems, system components, or an external provider.

Discussion for Enterprise Architecture | Offloading (PM-7(1))
Not every function or service that a system provides is essential to organizational mission or business functions. Printing or copying is an example of a non-essential but supporting service for an organization. Whenever feasible, such supportive but non-essential functions or services are not co-located with the functions or services that support essential mission or business functions. Maintaining such functions on the same system or system component increases the attack surface of the organization's mission-essential functions or services. Moving supportive but non-essential functions to a non-critical system, system component, or external provider can also increase efficiency by putting those functions or services under the control of individuals or providers who are subject matter experts in the functions or services.

Critical Infrastructure Plan (PM-8)

Description for Critical Infrastructure Plan (PM-8)
Address information security and privacy issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

Discussion for Critical Infrastructure Plan (PM-8)
Protection strategies are based on the prioritization of critical assets and resources. The requirement and guidance for defining critical infrastructure and key resources and for preparing an associated critical infrastructure protection plan are found in applicable laws, executive orders, directives, policies, regulations, standards, and guidelines.

Risk Management Strategy (PM-9)

Description for Risk Management Strategy (PM-9)
a. Develops 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;
b. Implement the risk management strategy consistently across the organization; and
c. Review and update the risk management strategy [Assignment: organization-defined frequency] or as required, to address organizational changes.

Discussion for Risk Management Strategy (PM-9)
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 across the organization with respect to the organization's risk tolerance, and approaches for monitoring risk over time. The senior accountable official for risk management (agency head or designated official) aligns information security management processes with strategic,

operational, 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 that the strategy is broad-based and comprehensive. The supply chain risk management strategy described in PM-30 can also provide useful inputs to the organization-wide risk management strategy.

Authorization Process (PM-10)

Description for Authorization Process (PM-10)
a. Manage the security and privacy state of organizational systems and the environments in which those systems operate through authorization processes;
b. Designate individuals to fulfill specific roles and responsibilities within the organizational risk management process; and
c. Integrate the authorization processes into an organization-wide risk management program.

Discussion for Authorization Process (PM-10)
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 officials for each organizational system and common control provider. The authorization processes for the organization 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.

Mission and Business Process Definition (PM-11)

Description for Mission and Business Process Definition (PM-11)
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].

Discussion for Mission and Business Process Definition (PM-11)
Protection needs are technology-independent capabilities that are required to counter threats to organizations, individuals, systems, and the Nation through the compromise of information (i.e., loss of confidentiality, integrity, availability, or privacy). Information protection and personally identifiable information processing needs are derived from the mission and business needs defined by organizational stakeholders, the mission and business processes designed 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 to defining protection and personally identifiable information processing needs is an understanding of the adverse impact that could result if a compromise or breach of information occurs. The categorization process is used to make 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 the processing of personally identifiable information at any stage of the information 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 policies and procedures.

Insider Threat Program (PM-12)

Description for Insider Threat Program (PM-12)
Implement an insider threat program that includes a cross-discipline insider threat incident handling team.

Discussion for Insider Threat Program (PM-12)
Organizations that handle classified information are required, under Executive Order 13587 EO 13587 and the National Insider Threat Policy ODNI NITP, to establish insider threat programs. The same standards and guidelines that apply to insider threat programs in classified environments can also 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 both technical and nontechnical information to identify potential insider threat concerns. A senior official is designated by the department or agency head as the responsible individual to implement and provide oversight for the program. In addition to the centralized integration and analysis capability, insider threat programs require organizations to prepare department or agency insider threat policies and implementation plans, conduct host-based user monitoring of individual employee activities on government-owned classified computers, provide insider threat awareness training to employees, receive access to information from offices in the department or agency for insider threat analysis, and conduct self-assessments of department or agency insider threat posture.
Insider threat programs can leverage the existence of incident handling teams that organizations may already have in place, such as computer security incident response teams. Human resources records are especially important in this effort, as there is compelling evidence to show that some types of insider crimes are often preceded by nontechnical behaviors in the workplace, including ongoing patterns of disgruntled behavior and conflicts with coworkers and other colleagues. These precursors can guide organizational officials in more focused, targeted monitoring efforts. However, the use of human resource records could raise significant concerns for privacy. The participation of a legal 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.

Security and Privacy Workforce (PM-13)

Description for Security and Privacy Workforce (PM-13)
Establish a security and privacy workforce development and improvement program.

Discussion for Security and Privacy Workforce (PM-13)
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 incumbents 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 fill 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 of personnel needed to protect organizational operations, assets, and individuals.

Testing, Training, and Monitoring (PM-14)

Description for Testing, Training, and Monitoring (PM-14)
a. Implement a process for ensuring that organizational plans for conducting security and privacy testing, training, and monitoring activities associated with organizational systems:
1. Are developed and maintained; and
2. Continue to be executed; and
b. Review testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

Discussion for Testing, Training, and Monitoring (PM-14)
A process for organization-wide security and privacy testing, training, and monitoring helps ensure that organizations provide oversight for testing, training, and monitoring activities and that those activities 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 consolidate the testing and monitoring activities that are routinely 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.

Security and Privacy Groups and Associations (PM-15)

Description for Security and Privacy Groups and Associations (PM-15)
Establish and institutionalize contact with selected groups and associations within the security and privacy communities:
a. To facilitate ongoing security and privacy education and training for organizational personnel;
b. To maintain currency with recommended security and privacy practices, techniques, and technologies; and
c. To share current security and privacy information, including threats, vulnerabilities, and incidents.

Discussion for Security and Privacy Groups and Associations (PM-15)
Ongoing 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, users' groups, and peer groups of security and privacy professionals in similar organizations. Organizations select security and privacy groups and associations based on mission and business functions. Organizations 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.

Threat Awareness Program (PM-16)

Description for Threat Awareness Program (PM-16)
Implement a threat awareness program that includes a cross-organization information-sharing capability for threat intelligence.

Discussion for Threat Awareness Program (PM-16)
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 this 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 are effective against certain types of threats, and threat intelligence (i.e., indications and warnings about threats). Threat information sharing may be bilateral or multilateral. Bilateral threat sharing includes government-to-commercial and government-to-government cooperatives. Multilateral threat sharing includes organizations taking part in threat-sharing consortia. Threat information may require special agreements and protection, or it may be freely shared.

Threat Awareness Program | Automated Means for Sharing Threat Intelligence (PM-16(1))

Description for Threat Awareness Program | Automated Means for Sharing Threat Intelligence (PM-16(1))
Employ automated mechanisms to maximize the effectiveness of sharing threat intelligence information.

Discussion for Threat Awareness Program | Automated Means for Sharing Threat Intelligence (PM-16(1))
To maximize the effectiveness of monitoring, it is important to know what threat observables and indicators the sensors need to be searching for. By using well-established frameworks, services, and automated tools, organizations improve their ability to rapidly share and feed the relevant threat detection signatures into monitoring tools.

Protecting Controlled Unclassified Information on External Systems (PM-17)

Description for Protecting Controlled Unclassified Information on External Systems (PM-17)
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; and
b. Review and update the policy and procedures [Assignment: organization-defined frequency].

Discussion for Protecting Controlled Unclassified Information on External Systems (PM-17)
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 and, specifically for systems external to the federal organization, 32 CFR 2002.14h. The policy prescribes the specific use and conditions to be implemented in accordance with organizational procedures, including via its contracting processes.

Privacy Program Plan (PM-18)

Description for Privacy Program Plan (PM-18)
a. Develop and disseminate an organization-wide privacy program plan that provides an overview of the agency'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;
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. Describes 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
b. Update the plan [Assignment: organization-defined frequency] and to address changes in federal privacy laws and policy and organizational changes and problems identified during plan implementation or privacy control assessments.

Discussion for Privacy Program Plan (PM-18)
A privacy program plan is a formal document that provides an overview of an 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 program 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, common, 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 selection operations explicitly or by reference) to enable control implementations 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. Together, the privacy plans for individual systems and the organization-wide privacy program plan 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.

Privacy Program Leadership Role (PM-19)

Description for Privacy Program Leadership Role (PM-19)
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 through the organization-wide privacy program.

Discussion for Privacy Program Leadership Role (PM-19)
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 roles on the data management board (see PM-23) and the data integrity board (see PM-24).

Dissemination of Privacy Program Information (PM-20)

Description for Dissemination of Privacy Program Information (PM-20)
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:
a. Ensures that the public has access to information about organizational privacy activities and can communicate with its senior agency official for privacy;
b. Ensures that organizational privacy practices and reports are publicly available; and
c. 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.

Discussion for Dissemination of Privacy Program Information (PM-20)
For federal agencies, the webpage is located at www.[agency].gov/privacy. Federal agencies include public privacy impact assessments, system of records notices, computer matching notices and agreements, PRIVACT exemption and implementation rules, privacy reports, privacy policies, instructions for individuals making an access or amendment request, email addresses for questions/complaints, blogs, and periodic publications.

Dissemination of Privacy Program Information | Privacy Policies on Websites, Applications, and Digital Services (PM-20(1))

Description for Dissemination of Privacy Program Information | Privacy Policies on Websites, Applications, and Digital Services (PM-20(1))
Develop and post privacy policies on all external-facing websites, mobile applications, and other digital services, that:
(a) Are written in plain language and organized in a way that is easy to understand and navigate;
(b) Provide information needed by the public to make an informed decision about whether and how to interact with the organization; and
(c) Are updated whenever the organization makes a substantive change to the practices it describes and includes a time/date stamp to inform the public of the date of the most recent changes.

Discussion for Dissemination of Privacy Program Information | Privacy Policies on Websites, Applications, and Digital Services (PM-20(1))
Organizations post privacy policies on all external-facing websites, mobile applications, and other digital services. Organizations post a link to the relevant privacy policy on any known, major entry points to the website, application, or digital service. In addition, organizations provide a link to the privacy policy on any webpage that collects personally identifiable information. Organizations may be subject to applicable laws, executive orders, directives, regulations, or policies that require the provision of specific information to the public. Organizational personnel consult with the senior agency official for privacy and legal counsel regarding such requirements.

Accounting of Disclosures (PM-21)

Description for Accounting of Disclosures (PM-21)
a. Develop and maintain an accurate accounting of disclosures of personally identifiable information, including:
1. Date, nature, and purpose of each disclosure; and
2. Name and address, or other contact information of the individual or organization to which the disclosure was made;
b. Retain the accounting of disclosures for the length of the time the personally identifiable information is maintained or five years after the disclosure is made, whichever is longer; and
c. Make the accounting of disclosures available to the individual to whom the personally identifiable information relates upon request.

Discussion for Accounting of Disclosures (PM-21)
The purpose of accounting of disclosures is to allow individuals to learn to whom their personally identifiable information has been disclosed, to provide a basis for subsequently advising recipients of any corrected or disputed personally identifiable information, and to provide an audit trail for subsequent reviews of 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 that provide notifications and alerts. Accounting of disclosures may also be used to help organizations verify compliance with applicable privacy statutes and policies governing the disclosure or dissemination of information and dissemination restrictions.

Personally Identifiable Information Quality Management (PM-22)

Description for Personally Identifiable Information Quality Management (PM-22)
Develop and document organization-wide policies and procedures for:
a. Reviewing for the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle;
b. Correcting or deleting inaccurate or outdated personally identifiable information;
c. Disseminating notice of corrected or deleted personally identifiable information to individuals or other appropriate entities; and
d. Appeals of adverse decisions on correction or deletion requests.

Discussion for Personally Identifiable Information Quality Management (PM-22)
Personally identifiable information quality management includes 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 involved 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 stigmatization. Correct information, in certain circumstances, can cause problems for individuals that outweigh the benefits of organizations maintaining the information. 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. Processes for correcting or deleting data are clearly defined and publicly available. Organizations use discretion in determining whether data is to be deleted or corrected based on the scope of requests, the changes sought, and the impact of the changes. Additionally, processes include the provision of responses to individuals of decisions to deny requests for correction or deletion. The responses include the reasons for the decisions, a means to record individual objections to the decisions, and a means of requesting reviews of the initial determinations.
Organizations notify individuals or their designated representatives when their personally identifiable information is corrected or deleted to provide transparency and confirm the completed action. Due to the complexity of data flows and storage, other entities may need to be informed of the correction or deletion. Notice supports the consistent correction and deletion of personally identifiable information across the data ecosystem.

Data Governance Body (PM-23)

Description for Data Governance Body (PM-23)
Establish a Data Governance Body consisting of [Assignment: organization-defined roles] with [Assignment: organization-defined responsibilities].

Discussion for Data Governance Body (PM-23)
A Data Governance Body can help ensure that the organization has coherent policies and the ability to balance the utility of data with security and privacy requirements. The Data Governance Body establishes policies, procedures, and standards that facilitate data governance so that data, including personally identifiable information, is effectively managed and maintained in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidance. Responsibilities can include developing and implementing guidelines that support data modeling, quality, integrity, and the de-identification needs of personally identifiable information across the information life cycle as well as reviewing and approving applications to release data outside of the organization, archiving the applications and the released data, and performing post-release monitoring to ensure that the assumptions made as part of the data release continue to be valid. Members include the chief information officer, senior agency information security officer, and senior agency official for privacy. Federal agencies are required to establish a Data Governance Body with specific roles and responsibilities in accordance with the EVIDACT and policies set forth under OMB M-19-23.

Data Integrity Board (PM-24)

Description for Data Integrity Board (PM-24)
Establish a Data Integrity Board to:
a. Review proposals to conduct or participate in a matching program; and
b. Conduct an annual review of all matching programs in which the agency has participated.

Discussion for Data Integrity Board (PM-24)
A Data Integrity Board is the board of senior officials designated by the head of a federal agency and is responsible for, among other things, reviewing the agency's proposals to conduct or participate in a matching program and conducting an annual review of all matching programs in which the agency has participated. As a general matter, a matching program is a computerized comparison of records from two or more automated PRIVACT systems of records or an automated system of records and automated records maintained by a non-federal agency (or agent thereof). A matching program either pertains to Federal benefit programs or Federal personnel or payroll records. At a minimum, the Data Integrity Board includes the Inspector General of the agency, if any, and the senior agency official for privacy.

Minimization of Personally Identifiable Information Used in Testing, Training, and Research (PM-25)

Description for Minimization of Personally Identifiable Information Used in Testing, Training, and Research (PM-25)
a. Develop, document, and implement policies and procedures that address the use of personally identifiable information for internal testing, training, and research;
b. Limit or minimize the amount of personally identifiable information used for internal testing, training, and research purposes;
c. Authorize the use of personally identifiable information when such information is required for internal testing, training, and research; and
d. Review and update policies and procedures [Assignment: organization-defined frequency].

Discussion for Minimization of Personally Identifiable Information Used in Testing, Training, and Research (PM-25)
The use of personally identifiable information in testing, research, and training increases the risk of unauthorized disclosure or misuse of such information. Organizations consult with the senior agency official for privacy and/or legal counsel to ensure that the use of personally identifiable information in testing, training, and research is compatible with the original purpose for which it was collected. When possible, organizations use placeholder data to avoid exposure of personally identifiable information when conducting testing, training, and research.

Complaint Management (PM-26)

Description for Complaint Management (PM-26)
Implement a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational security and privacy practices that includes:
a. Mechanisms that are easy to use and readily accessible by the public;
b. All information necessary for successfully filing complaints;
c. Tracking mechanisms to ensure all complaints received are reviewed and addressed within [Assignment: organization-defined time period];
d. Acknowledgement of receipt of complaints, concerns, or questions from individuals within [Assignment: organization-defined time period]; and
e. Response to complaints, concerns, or questions from individuals within [Assignment: organization-defined time period].

Discussion for Complaint Management (PM-26)
Complaints, concerns, and questions from individuals can serve as valuable sources of input to organizations and ultimately improve operational models, uses of technology, data collection practices, and controls. Mechanisms that can be used by the public include telephone hotline, email, or web-based forms. The information necessary for successfully filing complaints includes contact information for the senior agency official for privacy or other official designated to receive complaints. Privacy complaints may also include personally identifiable information which is handled in accordance with relevant policies and processes.

Privacy Reporting (PM-27)

Description for Privacy Reporting (PM-27)
a. Develop [Assignment: organization-defined privacy reports] and disseminate to:
1. [Assignment: organization-defined oversight bodies] to demonstrate accountability with statutory, regulatory, and policy privacy mandates; and
2. [Assignment: organization-defined officials] and other personnel with responsibility for monitoring privacy program compliance; and
b. Review and update privacy reports [Assignment: organization-defined frequency].

Discussion for Privacy Reporting (PM-27)
Through internal and external reporting, organizations promote accountability and transparency in organizational privacy operations. Reporting can also help organizations to determine progress in meeting privacy compliance requirements and privacy controls, compare performance across the federal government, discover vulnerabilities, identify gaps in policy and implementation, and identify models for success. For federal agencies, privacy reports include annual senior agency official for privacy reports to OMB, reports to Congress required by Implementing Regulations of the 9/11 Commission Act, and other public reports required by law, regulation, or policy, including internal policies of organizations. The senior agency official for privacy consults with legal counsel, where appropriate, to ensure that organizations meet all applicable privacy reporting requirements.

Risk Framing (PM-28)

Description for Risk Framing (PM-28)
a. Identify and document:
1. Assumptions affecting risk assessments, risk responses, and risk monitoring;
2. Constraints affecting risk assessments, risk responses, and risk monitoring;
3. Priorities and trade-offs considered by the organization for managing risk; and
4. Organizational risk tolerance;
b. Distribute the results of risk framing activities to [Assignment: organization-defined personnel]; and
c. Review and update risk framing considerations [Assignment: organization-defined frequency].

Discussion for Risk Framing (PM-28)
Risk framing is most effective when conducted at the organization level and in consultation with stakeholders throughout the organization including mission, business, and system owners. The assumptions, constraints, risk tolerance, priorities, and trade-offs identified as part of the risk framing process inform the risk management strategy, which in turn informs the conduct of risk assessment, risk response, and risk monitoring activities. Risk framing results are shared with organizational personnel, including mission and business owners, information owners or stewards, system owners, authorizing officials, senior agency information security officer, senior agency official for privacy, and senior accountable official for risk management.

Risk Management Program Leadership Roles (PM-29)

Description for Risk Management Program Leadership Roles (PM-29)
a. Appoint a Senior Accountable Official for Risk Management to align organizational information security and privacy management processes with strategic, operational, and budgetary planning processes; and
b. Establish a Risk Executive (function) to view and analyze risk from an organization-wide perspective and ensure management of risk is consistent across the organization.

Discussion for Risk Management Program Leadership Roles (PM-29)
The senior accountable official for risk management leads the risk executive (function) in organization-wide risk management activities.

Supply Chain Risk Management Strategy (PM-30)

Description for Supply Chain Risk Management Strategy (PM-30)
a. 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;
1. Implement the supply chain risk management strategy consistently across the organization; and
(a) Review and update the supply chain risk management strategy on [Assignment: organization-defined frequency] or as required, to address organizational changes.

Discussion for Supply Chain Risk Management Strategy (PM-30)
An organization-wide supply chain risk management strategy includes an unambiguous expression of the supply chain risk appetite and tolerance for the organization, acceptable supply chain risk mitigation strategies or controls, a process for consistently evaluating and monitoring supply chain risk, approaches for implementing and communicating the supply chain risk management strategy, and the associated roles and responsibilities. Supply chain risk management includes considerations of the security and privacy risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services. The supply chain risk management strategy can

be incorporated into the organization's overarching risk management strategy and can guide and inform supply chain policies and system-level supply chain risk management plans. In addition, the use of a risk executive function can facilitate a consistent, organization-wide application of the supply chain risk management strategy. The supply chain risk management strategy is implemented at the organization and mission/business levels, whereas the supply chain risk management plan (see SR-2) is implemented at the system level.

Supply Chain Risk Management Strategy | Suppliers of Critical or Mission-essential Items (PM-30(1))

Description for Supply Chain Risk Management Strategy | Suppliers of Critical or Mission-essential Items (PM-30(1))
Identify, prioritize, and assess suppliers of critical or mission-essential technologies, products, and services.

Discussion for Supply Chain Risk Management Strategy | Suppliers of Critical or Mission-essential Items (PM-30(1))
The identification and prioritization of suppliers of critical or mission-essential technologies, products, and services is paramount to the mission/business success of organizations. The assessment of suppliers is conducted using supplier reviews (see SR-6) and supply chain risk assessment processes (see RA-3(1)). An analysis of supply chain risk can help an organization identify systems or components for which additional supply chain risk mitigations are required.

Continuous Monitoring Strategy (PM-31)

Description for Continuous Monitoring Strategy (PM-31)
Develop an organization-wide continuous monitoring strategy and implement continuous monitoring programs that include:
a. Establishing the following organization-wide metrics to be monitored: [Assignment: organization-defined metrics];
b. Establishing [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessment of control effectiveness;
c. Ongoing monitoring of organizationally-defined metrics in accordance with the continuous monitoring strategy;
d. Correlation and analysis of information generated by control assessments and monitoring;
e. Response actions to address results of the analysis of control assessment and monitoring information; and
f. Reporting the security and privacy status of organizational systems to [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency].

Discussion for Continuous Monitoring Strategy (PM-31)
Continuous monitoring at the organization level facilitates ongoing awareness of the security and privacy posture across the organization to support organizational risk management decisions. The terms continuous and ongoing imply that organizations assess and monitor their controls and risks at a frequency sufficient to support risk-based decisions. Different types of controls may require different monitoring frequencies. The results of continuous monitoring guide and inform risk response actions by organizations. Continuous monitoring programs allow organizations to maintain the authorizations of systems and common controls in highly dynamic environments of operation with changing mission and business needs, threats, vulnerabilities, and technologies. Having access to security- and privacy-related information on a continuing basis through reports and dashboards gives organizational officials the capability to make effective, timely, and informed risk management decisions, including ongoing authorization decisions. To further facilitate security and privacy risk management, organizations consider aligning organization-defined monitoring metrics with organizational risk tolerance as defined in the risk management strategy. Monitoring requirements, including the need for monitoring, may be referenced in other controls and control enhancements such as, 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), CA-7, CM-3f, CM-6d, CM-11c, IR-5, MA-2b, MA-3a, MA-4a, PE-3d, PE-6, PE-14b, PE-16, PE-20, PM-6, PM-23, PS-7e, SA-9c, SC-5(3)(b), SC-7a, SC-7(24)(b), SC-18b, SC-43b, SI-4.

Purposing (PM-32)

Description for Purposing (PM-32)
Analyze [Assignment: organization-defined systems or systems components] supporting mission essential services or functions to ensure that the information resources are being used consistent with their intended purpose.

Discussion for Purposing (PM-32)
Systems are designed to support a specific mission or business function. However, over time, systems and system components may be used to support services and functions that are outside of the scope of the intended mission or business functions. This can result in exposing information resources to unintended environments and uses that can significantly increase threat exposure. In doing so, the systems are more vulnerable to compromise, which can ultimately impact the services and functions for which they were intended. This is especially impactful for mission-essential services and functions. By analyzing resource use, organizations can identify such potential exposures.

Policy and Procedures (PS-1)

Description for Policy and Procedures (PS-1)
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] personnel security policy that:
(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the personnel security policy and the associated personnel security controls;
b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the personnel security policy and procedures; and
c. Review and update the current personnel security:
1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

Discussion for Policy and Procedures (PS-1)
Personnel security policy and procedures for the controls in the PS family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to 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 mission level or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies reflecting the complex nature of organizations. Procedures can be established for security and privacy programs, for mission/business processes, 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. Events that may precipitate an update to personnel security policy and procedures include, but are not limited to, assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Position Risk Designation (PS-2)

Description for Position Risk Designation (PS-2)
a. Assign a risk designation to all organizational positions;
b. Establish screening criteria for individuals filling those positions; and
c. Review and update position risk designations [Assignment: organization-defined frequency].

Discussion for Position Risk Designation (PS-2)
Position risk designations reflect Office of Personnel Management (OPM) policy and guidance. Proper position designation is the foundation of an effective and consistent suitability and personnel security program. The Position Designation System (PDS) assesses the duties and responsibilities of a position to determine the degree of potential damage to the efficiency or integrity of the service due to misconduct of an incumbent of a position and establishes the risk level of that position. The PDS assessment also determines if the duties and responsibilities of the position present the potential for position incumbents to bring about a material adverse effect on national security and the degree of that potential effect, which establishes the sensitivity level of a position. The results of the assessment determine what level of investigation is conducted for a position. Risk designations can guide and inform the types of authorizations that individuals receive when accessing organizational information and information systems. Position screening criteria include explicit information security role appointment requirements. Parts 1400 and 731 of Title 5, Code of Federal Regulations, establish the requirements for organizations to evaluate relevant covered positions for a position sensitivity and position risk designation commensurate with the duties and responsibilities of those positions.

Personnel Screening (PS-3)

Description for Personnel Screening (PS-3)
a. Screen individuals prior to authorizing access to the system; and
b. Rescreen individuals in accordance with [Assignment: organization-defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of rescreening].

Discussion for Personnel Screening (PS-3)
Personnel screening and rescreening activities reflect applicable laws, executive orders, directives, regulations, policies, standards, guidelines, and specific criteria established for the risk designations of assigned positions. Examples of personnel screening include background investigations and agency checks. Organizations may define different rescreening conditions and frequencies for personnel accessing systems based on types of information processed, stored, or transmitted by the systems.

Personnel Screening | Classified Information (PS-3(1))

Description for Personnel Screening | Classified Information (PS-3(1))
Verify that individuals accessing a system processing, storing, or transmitting classified information are cleared and indoctrinated to the highest classification level of the information to which they have access on the system.

Discussion for Personnel Screening | Classified Information (PS-3(1))
Classified information is the most sensitive information that the Federal Government processes, stores, or transmits. It is imperative that individuals have the requisite security clearances and system access authorizations prior to gaining access to such information. Access authorizations are enforced by system access controls (see AC-3) and flow controls (see AC-4).

Personnel Screening | Formal Indoctrination (PS-3(2))

Description for Personnel Screening | Formal Indoctrination (PS-3(2))
Verify that individuals accessing a system processing, storing, or transmitting types of classified information that require formal indoctrination, are formally indoctrinated for all the relevant types of information to which they have access on the system.

Discussion for Personnel Screening | Formal Indoctrination (PS-3(2))
Types of classified information that require formal indoctrination include Special Access Program (SAP), Restricted Data (RD), and Sensitive Compartmented Information (SCI).

Personnel Screening | Information Requiring Special Protective Measures (PS-3(3))

Description for Personnel Screening | Information Requiring Special Protective Measures (PS-3(3))
Verify that individuals accessing a system processing, storing, or transmitting information requiring special protection:
(a) Have valid access authorizations that are demonstrated by assigned official government duties; and
(b) Satisfy [Assignment: organization-defined additional personnel screening criteria].

Discussion for Personnel Screening | Information Requiring Special Protective Measures (PS-3(3))
Organizational information that requires special protection includes controlled unclassified information. Personnel security criteria include position sensitivity background screening requirements.

Personnel Screening | Citizenship Requirements (PS-3(4))

Description for Personnel Screening | Citizenship Requirements (PS-3(4))
Verify that individuals accessing a system processing, storing, or transmitting [Assignment: organization-defined information types] meet [Assignment: organization-defined citizenship requirements].

Discussion for Personnel Screening | Citizenship Requirements (PS-3(4))
None.

Personnel Termination (PS-4)

Description for Personnel Termination (PS-4)
Upon termination of individual employment:
a. Disable system access within [Assignment: organization-defined time period];
b. Terminate or revoke any authenticators and credentials associated with the individual;
c. Conduct exit interviews that include a discussion of [Assignment: organization-defined information security topics];
d. Retrieve all security-related organizational system-related property; and
e. Retain access to organizational information and systems formerly controlled by terminated individual.

Discussion for Personnel Termination (PS-4)
System property includes hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes. Exit interviews ensure that terminated individuals understand the security constraints imposed by being former employees and that proper accountability is achieved for system-related property. Security topics at exit interviews include reminding individuals of nondisclosure agreements and potential limitations on future employment. Exit interviews may not always be possible for some individuals, including in cases related to the unavailability of supervisors, illnesses, or job abandonment. Exit interviews are important for individuals with security clearances. The timely execution of termination actions is essential for individuals who have been terminated for cause. In certain situations, organizations consider disabling the system accounts of individuals who are being terminated prior to the individuals being notified.

Personnel Termination | Post-employment Requirements (PS-4(1))

Description for Personnel Termination | Post-employment Requirements (PS-4(1))
(a) Notify terminated individuals of applicable, legally binding post-employment requirements for the protection of organizational information; and
(b) Require terminated individuals to sign an acknowledgment of post-employment requirements as part of the organizational termination process.

Discussion for Personnel Termination | Post-employment Requirements (PS-4(1))
Organizations consult with the Office of the General Counsel regarding matters of post-employment requirements on terminated individuals.

Personnel Termination | Automated Actions (PS-4(2))

Description for Personnel Termination | Automated Actions (PS-4(2))
Use [Assignment: organization-defined automated mechanisms] to [Selection (one or more): notify [Assignment: organization-defined personnel or roles] of individual termination actions; disable access to system resources].

Discussion for Personnel Termination | Automated Actions (PS-4(2))
In organizations with many employees, not all personnel who need to know about termination actions receive the appropriate notifications, or if such notifications are received, they may not occur in a timely manner. Automated mechanisms can be used to send automatic alerts or notifications to organizational personnel or roles when individuals are terminated. Such automatic alerts or notifications can be conveyed in a variety of ways, including via telephone, electronic mail, text message, or websites. Automated mechanisms can also be employed to quickly

and thoroughly disable access to system resources after an employee is terminated.

Personnel Transfer (PS-5)

Description for Personnel Transfer (PS-5)
a. Review and confirm ongoing operational need for current logical and physical access authorizations to systems and facilities when individuals are reassigned or transferred to other positions within the organization;
b. Initiate [Assignment: organization-defined transfer or reassignment actions] within [Assignment: organization-defined time period following the formal transfer action];
c. Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and
d. Notify [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period].

Discussion for Personnel Transfer (PS-5)
Personnel transfer applies when reassignments or transfers of individuals are permanent or of such extended duration as to make the actions warranted. Organizations define actions appropriate for the types of reassignments or transfers, whether permanent or extended. Actions that may be required for personnel transfers or reassignments to other positions within organizations include returning old and issuing new keys, identification cards, and building passes; closing system accounts and establishing new accounts; changing system access authorizations (i.e., privileges); and providing for access to official records to which individuals had access at previous work locations and in previous system accounts.

Access Agreements (PS-6)

Description for Access Agreements (PS-6)
a. Develop and document access agreements for organizational systems;
b. Review and update the access agreements [Assignment: organization-defined frequency]; and
c. Verify that individuals requiring access to organizational information and systems:
1. Sign appropriate access agreements prior to being granted access; and
2. Re-sign access agreements to maintain access to organizational systems when access agreements have been updated or [Assignment: organization-defined frequency].

Discussion for Access Agreements (PS-6)
Access agreements include nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Signed access agreements include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with organizational systems to which access is authorized. Organizations can use electronic signatures to acknowledge access agreements unless specifically prohibited by organizational policy.

Access Agreements | Information Requiring Special Protection (PS-6(1))

Description for Access Agreements | Information Requiring Special Protection (PS-6(1))
[Withdrawn: Incorporated into PS-3.]

Discussion for Access Agreements | Information Requiring Special Protection (PS-6(1))

Access Agreements | Classified Information Requiring Special Protection (PS-6(2))

Description for Access Agreements | Classified Information Requiring Special Protection (PS-6(2))
Verify that access to classified information requiring special protection is granted only to individuals who:
(a) Have a valid access authorization that is demonstrated by assigned official government duties;
(b) Satisfy associated personnel security criteria; and
(c) Have read, understood, and signed a nondisclosure agreement.

Discussion for Access Agreements | Classified Information Requiring Special Protection (PS-6(2))
Classified information that requires special protection includes collateral information, Special Access Program (SAP) information, and Sensitive Compartmented Information (SCI). Personnel security criteria reflect applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Access Agreements | Post-employment Requirements (PS-6(3))

Description for Access Agreements | Post-employment Requirements (PS-6(3))
(a) Notify individuals of applicable, legally binding post-employment requirements for protection of organizational information; and
(b) Require individuals to sign an acknowledgment of these requirements, if applicable, as part of granting initial access to covered information.

Discussion for Access Agreements | Post-employment Requirements (PS-6(3))
Organizations consult with the Office of the General Counsel regarding matters of post-employment requirements on terminated individuals.

External Personnel Security (PS-7)

Description for External Personnel Security (PS-7)
a. Establish personnel security requirements, including security roles and responsibilities for external providers;
b. Require external providers to comply with personnel security policies and procedures established by the organization;
c. Document personnel security requirements;
d. Require external providers to notify [Assignment: organization-defined personnel or roles] of any personnel transfers or terminations of external personnel who possess organizational credentials and/or badges, or who have system privileges within [Assignment: organization-defined time period]; and
e. Monitor provider compliance with personnel security requirements.

Discussion for External Personnel Security (PS-7)
External provider refers to organizations other than the organization operating or acquiring the system. External providers include service bureaus, contractors, and other organizations that provide system development, information technology services, testing or assessment services, outsourced applications, and network/security management. Organizations explicitly include personnel security requirements in acquisition-related documents. External providers may have personnel working at organizational facilities with credentials, badges, or system privileges issued by organizations. Notifications of external personnel changes ensure the appropriate termination of privileges and credentials. Organizations define the transfers and terminations deemed reportable by security-related characteristics that include functions, roles, and the nature of credentials or privileges associated with transferred or terminated individuals.

Personnel Sanctions (PS-8)

Description for Personnel Sanctions (PS-8)
a. Employ a formal sanctions process for individuals failing to comply with established information security and privacy policies and procedures; and
b. Notify [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period] when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

Discussion for Personnel Sanctions (PS-8)
Organizational sanctions reflect applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Sanctions processes are described in access agreements and can be included as part of general personnel policies for organizations and/or specified in security and privacy policies. Organizations consult with the Office of the General Counsel regarding matters of employee sanctions.

Position Descriptions (PS-9)

Description for Position Descriptions (PS-9)
Incorporate security and privacy roles and responsibilities into organizational position descriptions.

Discussion for Position Descriptions (PS-9)
Specification of security and privacy roles in individual organizational position descriptions facilitates clarity in understanding the security or privacy responsibilities associated with the roles and the role-based security and privacy training requirements for the roles.

Policy and Procedures (PT-1)

Description for Policy and Procedures (PT-1)
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] personally identifiable information processing and transparency policy that:
(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the personally identifiable information processing and transparency policy and the associated personally identifiable information processing and transparency controls;
b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the personally identifiable information processing and transparency policy and procedures; and
c. Review and update the current personally identifiable information processing and transparency:
1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

Discussion for Policy and Procedures (PT-1)
Personally identifiable information processing and transparency policy and procedures address the controls in the PT family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of personally identifiable information processing and transparency policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, 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. Events that may precipitate an update to personally identifiable information processing and transparency policy and procedures include assessment or audit findings,

breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Authority to Process Personally Identifiable Information (PT-2)

Description for Authority to Process Personally Identifiable Information (PT-2)
a. Determine and document the [Assignment: organization-defined authority] that permits the [Assignment: organization-defined processing] of personally identifiable information; and
b. Restrict the [Assignment: organization-defined processing] of personally identifiable information to only that which is authorized.

Discussion for Authority to Process Personally Identifiable Information (PT-2)
The processing of personally identifiable information is an operation or set of operations that the information system or organization performs with respect to personally identifiable information across the information life cycle. Processing includes but is not limited to creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal. Processing operations also include logging, generation, and transformation, as well as analysis techniques, such as data mining.
Organizations may be subject to laws, executive orders, directives, regulations, or policies that establish the organization's authority and thereby limit certain types of processing of personally identifiable information or establish other requirements related to the processing. Organizational personnel consult with the senior agency official for privacy and legal counsel regarding such authority, particularly if the organization is 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 they process personally identifiable information. While processing of personally identifiable information may be legally permissible, privacy risks may still arise. 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 this 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 other documentation.
Organizations take steps to ensure that personally identifiable information is only processed 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.

Authority to Process Personally Identifiable Information | Data Tagging (PT-2(1))

Description for Authority to Process Personally Identifiable Information | Data Tagging (PT-2(1))
Attach data tags containing [Assignment: organization-defined authorized processing] to [Assignment: organization-defined elements of personally identifiable information].

Discussion for Authority to Process Personally Identifiable Information | Data Tagging (PT-2(1))
Data tags support the 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.

Authority to Process Personally Identifiable Information | Automation (PT-2(2))

Description for Authority to Process Personally Identifiable Information | Automation (PT-2(2))
Manage enforcement of the authorized processing of personally identifiable information using [Assignment: organization-defined automated mechanisms].

Discussion for Authority to Process Personally Identifiable Information | Automation (PT-2(2))
Automated mechanisms augment verification that only authorized processing is occurring.

Personally Identifiable Information Processing Purposes (PT-3)

Description for Personally Identifiable Information Processing Purposes (PT-3)
a. Identify and document the [Assignment: organization-defined purpose(s)] for processing personally identifiable information;
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(s); and
d. Monitor changes in processing personally identifiable information and implement [Assignment: organization-defined mechanisms] to ensure that any changes are made in accordance with [Assignment: organization-defined requirements].

Discussion for Personally Identifiable Information Processing Purposes (PT-3)
Identifying and documenting the purpose for processing provides organizations with a basis for understanding why personally identifiable information may be processed. The term process includes every step of the information life cycle, including creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal. Identifying and documenting the purpose of processing is a prerequisite to enabling owners and operators of the system and individuals whose information is processed by the system to understand how the information will be processed. This enables individuals to make informed decisions about their engagement with information systems and organizations and to manage their privacy interests. Once the specific processing purpose has been identified, the purpose is described in the organization's privacy notices, policies, and any related privacy compliance documentation, including privacy impact

assessments, system of records notices, PRIVACT statements, computer matching notices, and other applicable Federal Register notices.

Organizations take steps to help ensure that personally identifiable information is processed only for identified purposes, including training organizational personnel and monitoring and auditing organizational processing of personally identifiable information.

Organizations monitor for changes in personally identifiable information processing. Organizational personnel consult with the senior agency official for privacy and legal counsel to ensure that any new purposes that arise from changes in processing are compatible with the purpose for which the information was collected, or if the new purpose is not compatible, implement mechanisms in accordance with defined requirements to allow for the new processing, if appropriate. Mechanisms may include obtaining consent from individuals, revising privacy policies, or other measures to manage privacy risks that arise from changes in personally identifiable information processing purposes.

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

Description for Personally Identifiable Information Processing Purposes | Data Tagging (PT-3(1))
Attach data tags containing the following purposes to [Assignment: organization-defined elements of personally identifiable information]: [Assignment: organization-defined processing purposes].

Discussion for Personally Identifiable Information Processing Purposes | Data Tagging (PT-3(1))
Data tags support the tracking of processing purposes by conveying the purposes 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 as the information transits a system, a system owner or operator can identify whether a change in processing would be compatible with the identified and documented purposes. Data tags may also support the use of automated tools.

Personally Identifiable Information Processing Purposes | Automation (PT-3(2))

Description for Personally Identifiable Information Processing Purposes | Automation (PT-3(2))
Track processing purposes of personally identifiable information using [Assignment: organization-defined automated mechanisms].

Discussion for Personally Identifiable Information Processing Purposes | Automation (PT-3(2))
Automated mechanisms augment tracking of the processing purposes.

Consent (PT-4)

Description for Consent (PT-4)
Implement [Assignment: organization-defined tools or mechanisms] for individuals to consent to the processing of their personally identifiable information prior to its collection that facilitate individuals' informed decision-making.

Discussion for Consent (PT-4)
Consent allows individuals to participate in making decisions 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. Consent may be required by applicable laws, executive orders, directives, regulations, policies, standards, or guidelines. Otherwise, when selecting consent as a control, organizations consider whether individuals can be reasonably expected to understand and accept the privacy risks that arise from their authorization. Organizations consider whether other controls may more effectively mitigate privacy risk either alone or in conjunction with consent. Organizations also consider any demographic or contextual factors that may influence the understanding or behavior of individuals with respect to the processing carried out by the system or organization. When soliciting consent from individuals, organizations consider the appropriate mechanism for obtaining consent, including the type of consent (e.g., opt-in, opt-out), how to properly authenticate and identity 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.

Consent | Tailored Consent (PT-4(1))

Description for Consent | Tailored Consent (PT-4(1))
Provide [Assignment: organization-defined mechanisms] to allow individuals to tailor processing permissions to selected elements of personally identifiable information.

Discussion for Consent | Tailored Consent (PT-4(1))
While some processing may be necessary for the basic functionality of the product or service, other processing may not. In these circumstances, organizations allow individuals to select how specific personally identifiable information elements may be processed. More tailored consent may help reduce privacy risk, increase individual satisfaction, and avoid adverse behaviors, such as abandonment of the product or service.

Consent | Just-in-time Consent (PT-4(2))

Description for Consent | Just-in-time Consent (PT-4(2))
Present [Assignment: organization-defined consent mechanisms] to individuals at [Assignment: organization-defined frequency] and in conjunction with [Assignment: organization-defined personally identifiable information processing].

Discussion for Consent | Just-in-time Consent (PT-4(2))
Just-in-time consent enables individuals to participate in how their personally identifiable information is being processed at the time or in conjunction with specific types of data processing when such participation may be most useful to the individual. Individual assumptions about how personally identifiable information is being processed might not be accurate or reliable if time has passed since the individual last gave consent or the type of processing creates significant privacy risk. Organizations use discretion to determine when to use just-in-time consent and may use supporting information on demographics, focus groups, or surveys to learn more about individuals' privacy interests and concerns.

Consent | Revocation (PT-4(3))

Description for Consent | Revocation (PT-4(3))
Implement [Assignment: organization-defined tools or mechanisms] for individuals to revoke consent to the processing of their personally identifiable information.

Discussion for Consent | Revocation (PT-4(3))
Revocation of consent enables individuals to exercise control over their initial consent decision when circumstances change. Organizations consider usability factors in enabling easy-to-use revocation capabilities.

Privacy Notice (PT-5)

Description for Privacy Notice (PT-5)
Provide notice to individuals about the processing of personally identifiable information that:
a. Is available to individuals upon first interacting with an organization, and subsequently at [Assignment: organization-defined frequency];
b. Is clear and easy-to-understand, expressing information about personally identifiable information processing in plain language;
c. Identifies the authority that authorizes the processing of personally identifiable information;
d. Identifies the purposes for which personally identifiable information is to be processed; and
e. Includes [Assignment: organization-defined information].

Discussion for Privacy Notice (PT-5)
Privacy notices help inform individuals about how their personally identifiable information is being processed by the system or organization. Organizations use privacy notices to inform individuals about how, under what authority, and for what purpose their personally identifiable information is processed, as well as other information such as choices individuals might have with respect to that processing and other parties with whom information is shared. Laws, executive orders, directives, regulations, or policies may require that privacy notices include specific elements or be provided in specific formats. Federal agency personnel consult with the senior agency official for privacy and legal counsel regarding when and where to provide privacy notices, as well as elements to include in privacy notices and required formats. In circumstances where laws or government-wide policies do not require privacy notices, organizational policies and determinations may require privacy notices and may serve as a source of the elements to include in privacy notices.
Privacy risk assessments identify the privacy risks associated with the processing of personally identifiable information and may help organizations determine appropriate elements to include in a privacy notice to manage such risks. To help individuals understand how their information is being processed, organizations write materials in plain language and avoid technical jargon.

Privacy Notice | Just-in-time Notice (PT-5(1))

Description for Privacy Notice | Just-in-time Notice (PT-5(1))
Present notice of personally identifiable information processing to individuals at a time and location where the individual provides personally identifiable information or in conjunction with a data action, or [Assignment: organization-defined frequency].

Discussion for Privacy Notice | Just-in-time Notice (PT-5(1))
Just-in-time notices inform individuals of how organizations process their personally identifiable information at a time when such notices may be most useful to the individuals. Individual assumptions about how personally identifiable information will be processed might not be accurate or reliable if time has passed since the organization last presented notice or the circumstances under which the individual was last provided notice have changed. A just-in-time notice can explain data actions that organizations have identified as potentially giving rise to greater privacy risk for individuals. Organizations can use a just-in-time notice to update or remind individuals about specific data actions as they occur or highlight specific changes that occurred since last presenting notice. A just-in-time notice can be used in conjunction with just-in-time consent to explain what will occur if consent is declined. Organizations use discretion to determine when to use a just-in-time notice and may use supporting information on user demographics, focus groups, or surveys to learn about users' privacy interests and concerns.

Privacy Notice | Privacy Act Statements (PT-5(2))

Description for Privacy Notice | Privacy Act Statements (PT-5(2))
Include Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Discussion for Privacy Notice | Privacy Act Statements (PT-5(2))
If a federal agency asks individuals to supply information that will become part of a system of records, the agency is required to provide a PRIVACT statement on the form used to collect the information or on a separate form that can be retained by the individual. The agency provides a PRIVACT statement in such circumstances regardless of whether the information will be collected on a paper or electronic form, on a website, on a mobile application, over the telephone, or through some other medium. This requirement ensures that the individual is provided with sufficient information about the request for information to make an informed decision on whether or not to respond.
PRIVACT statements provide formal notice to individuals of the authority that authorizes the solicitation of the information; whether providing the information is mandatory or voluntary; the principal purpose(s) for which the information is to be used; the published routine uses to which the information is subject; the effects on the individual, if any, of not providing all or any part of the information requested; and an appropriate citation and link to the relevant system of records notice.
Federal agency personnel consult with the senior agency official for privacy and legal counsel regarding the notice provisions of the PRIVACT.

System of Records Notice (PT-6)

Description for System of Records Notice (PT-6)
For systems that process information that will be maintained in a Privacy Act system of records:
a. Draft system of records notices in accordance with OMB guidance and submit new and significantly modified system of records notices to the OMB and appropriate congressional committees for advance review;
b. Publish system of records notices in the Federal Register; and
c. Keep system of records notices accurate, up-to-date, and scoped in accordance with policy.

Discussion for System of Records Notice (PT-6)
The PRIVACT requires that federal agencies publish a system of records notice in the Federal Register upon the establishment and/or modification of a PRIVACT 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 information 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 records, 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 OMB A-108.

System of Records Notice | Routine Uses (PT-6(1))

Description for System of Records Notice | Routine Uses (PT-6(1))
Review all routine uses published in the system of records notice at [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.

Discussion for System of Records Notice | Routine Uses (PT-6(1))
A PRIVACT routine use is a particular kind of disclosure of a record outside of the federal agency maintaining the system of records. A routine use is an exception to the PRIVACT prohibition on the disclosure of a record in a system of records without the prior written consent of the individual to whom the record pertains. To qualify as a routine use, the disclosure must be for a purpose that is compatible with the purpose for which the information was originally collected. The PRIVACT requires agencies to describe each routine use of the records maintained in the system of records, including the categories of users of the records and the purpose of the use. Agencies may only establish routine uses by explicitly publishing them in the relevant system of records notice.

System of Records Notice | Exemption Rules (PT-6(2))

Description for System of Records Notice | Exemption Rules (PT-6(2))
Review all Privacy Act exemptions claimed for the system of records at [Assignment: organization-defined frequency] to ensure they remain appropriate and necessary in accordance with law, that they have been promulgated as regulations, and that they are accurately described in the system of records notice.

Discussion for System of Records Notice | Exemption Rules (PT-6(2))
The PRIVACT includes two sets of provisions that allow federal agencies to claim exemptions from certain requirements in the statute. In certain circumstances, these provisions allow agencies to promulgate regulations to exempt a system of records from select provisions of the PRIVACT. At a minimum, organizations' PRIVACT exemption regulations include the specific name(s) of any system(s) of records that will be exempt, the specific provisions of the PRIVACT from which the system(s) of records is to be exempted, the reasons for the exemption, and an explanation for why the exemption is both necessary and appropriate.

Specific Categories of Personally Identifiable Information (PT-7)

Description for Specific Categories of Personally Identifiable Information (PT-7)
Apply [Assignment: organization-defined processing conditions] for specific categories of personally identifiable information.

Discussion for Specific Categories of Personally Identifiable Information (PT-7)
Organizations apply any conditions or protections that may be necessary for specific categories of personally identifiable information. These conditions may be required by laws, executive orders, directives, regulations, policies, standards, or guidelines. The requirements may also come from the results of privacy risk assessments that factor in contextual changes that may result in an organizational determination that a particular category of personally identifiable information is particularly sensitive or raises particular privacy risks. Organizations consult with the senior agency official for privacy and legal counsel regarding any protections that may be necessary.

Specific Categories of Personally Identifiable Information | Social Security Numbers (PT-7(1))

Description for Specific Categories of Personally Identifiable Information | Social Security Numbers (PT-7(1))
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 deny any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his or her Social Security number; and
(c) Inform any individual who is asked to disclose his or her Social Security number whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.

Discussion for Specific Categories of Personally Identifiable Information | Social Security Numbers (PT-7(1))
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.

Specific Categories of Personally Identifiable Information | First Amendment Information (PT-7(2))

Description for Specific Categories of Personally Identifiable Information | First Amendment Information (PT-7(2))
Prohibit the processing of information describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual or unless pertinent to and within the scope of an authorized law enforcement activity.

Discussion for Specific Categories of Personally Identifiable Information | First Amendment Information (PT-7(2))
The PRIVACT 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.

Computer Matching Requirements (PT-8)

Description for Computer Matching Requirements (PT-8)
When a system or organization processes information for the purpose of conducting a matching program:
a. Obtain approval from the Data Integrity Board to conduct the matching program;
b. Develop and enter into a computer matching agreement;
c. Publish a matching notice in the Federal Register;
d. Independently verify the information produced by the matching program before taking adverse action against an individual, if required; and
e. Provide individuals with notice and an opportunity to contest the findings before taking adverse action against an individual.

Discussion for Computer Matching Requirements (PT-8)
The PRIVACT establishes requirements for federal and non-federal agencies if they engage in a matching program. In general, a matching program is a computerized comparison of records from two or more automated PRIVACT systems of records or an automated system of records and automated records maintained by a non-federal agency (or agent thereof). A matching program either pertains to federal benefit programs or federal personnel or payroll records. A federal benefit match is performed to determine or verify eligibility for payments under federal benefit programs or to recoup payments or delinquent debts under federal benefit programs. A matching program involves not just the matching activity itself but also the investigative follow-up and ultimate action, if any.

Policy and Procedures (RA-1)

Description for Policy and Procedures (RA-1)
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] risk assessment policy that:
(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls;
b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the risk assessment policy and procedures; and
c. Review and update the current risk assessment:
1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

Discussion for Policy and Procedures (RA-1)
Risk assessment policy and procedures address the controls in the RA family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of risk assessment policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies reflecting the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, 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. Events that may precipitate an update to risk assessment policy and procedures include assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Security Categorization (RA-2)

Description for Security Categorization (RA-2)
a. Categorize the system and information it processes, stores, and transmits;
b. Document the security categorization results, including supporting rationale, in the security plan for the system; and
c. Verify that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.

Discussion for Security Categorization (RA-2)
Security categories describe the potential adverse impacts or negative consequences to organizational operations, organizational assets, and individuals if organizational information and systems are compromised through a loss of confidentiality, integrity, or availability. Security categorization is also a type of asset loss characterization in systems security engineering processes that is carried out throughout the system development life cycle. Organizations can use privacy risk assessments or privacy impact assessments to better understand the potential adverse effects on individuals. CNSSI 1253 provides additional guidance on categorization for national security systems.
Organizations conduct the security categorization process as an organization-wide activity with the direct involvement of chief information officers, senior agency information security officers, senior agency officials for privacy, system owners, mission and business owners, and information owners or stewards. Organizations consider the potential adverse impacts to other organizations and, in accordance with USA PATRIOT and Homeland Security Presidential Directives, potential national-level adverse impacts.
Security categorization processes facilitate the development of inventories of information assets and, along with CM-8, mappings to specific system components where information is processed, stored, or transmitted. The security categorization process is revisited throughout the system development life cycle to ensure that the security categories remain accurate and relevant.

Security Categorization | Impact-level Prioritization (RA-2(1))

Description for Security Categorization | Impact-level Prioritization (RA-2(1))
Conduct an impact-level prioritization of organizational systems to obtain additional granularity on system impact levels.

Discussion for Security Categorization | Impact-level Prioritization (RA-2(1))
Organizations apply the high-water mark concept to each system categorized in accordance with FIPS 199, resulting in systems designated as low impact, moderate impact, or high impact. Organizations that desire additional granularity in the system impact designations for risk-based decision-making, can further partition the systems into sub-categories of the initial system categorization. For example, an impact-level prioritization on a moderate-impact system can produce three new sub-categories: low-moderate systems, moderate-moderate systems, and high-moderate systems. Impact-level prioritization and the resulting sub-categories of the system give organizations an opportunity to focus their investments related to security control selection and the tailoring of control baselines in responding to identified risks. Impact-level prioritization can also be used to determine those systems that may be of heightened interest or value to adversaries or represent a critical loss to the federal enterprise, sometimes described as high value assets. For such high value assets, organizations may be more focused on complexity, aggregation, and information exchanges. Systems with high value assets can be prioritized by partitioning high-impact systems into low-high systems, moderate-high systems, and high-high systems. Alternatively, organizations can apply the guidance in CNSSI 1253 for security objective-related categorization.

Risk Assessment (RA-3)

Description for Risk Assessment (RA-3)
a. Conduct a risk assessment, including:
1. Identifying threats to and vulnerabilities in the system;
2. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and
3. Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information;
b. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments;
c. Document risk assessment results in [Selection: security and privacy plans; risk assessment report; [Assignment: organization-defined document]];
d. Review risk assessment results [Assignment: organization-defined frequency];
e. Disseminate risk assessment results to [Assignment: organization-defined personnel or roles]; and
f. Update the risk assessment [Assignment: organization-defined frequency] or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.

Discussion for Risk Assessment (RA-3)
Risk assessments consider threats, vulnerabilities, likelihood, and impact to organizational operations and assets, individuals, other organizations, and the Nation. Risk assessments also consider risk from external parties, including contractors who operate systems on behalf of the organization, individuals who access organizational systems, service providers, and outsourcing entities. Organizations can conduct risk assessments at all three levels in 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 also be conducted at various steps in the Risk Management Framework, including preparation, categorization, control selection, control implementation, control assessment, authorization, and control monitoring. Risk assessment is an ongoing activity carried out throughout the system development life cycle.
Risk assessments can also address information related to the system, including system design, the intended use of the system, testing results, and supply chain-related information or artifacts. Risk assessments can play an important role in control selection processes, particularly during the application of tailoring guidance and in the earliest phases of capability determination.

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

Description for Risk Assessment | Supply Chain Risk Assessment (RA-3(1))
(a) Assess supply chain risks associated with [Assignment: organization-defined systems, system components, and system services]; and
(b) 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.

Discussion for Risk Assessment | Supply Chain Risk Assessment (RA-3(1))
Supply chain-related events include disruption, use of defective components, insertion of counterfeits, theft, malicious development practices, improper delivery practices, and insertion 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, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. The supply chain-related events may 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.

Risk Assessment | Use of All-source Intelligence (RA-3(2))

Description for Risk Assessment | Use of All-source Intelligence (RA-3(2))
Use all-source intelligence to assist in the analysis of risk.

Discussion for Risk Assessment | Use of All-source Intelligence (RA-3(2))
Organizations employ all-source intelligence to inform engineering, acquisition, and risk management decisions. All-source intelligence consists of information derived from all available sources, including publicly available or open-source information, measurement and signature intelligence, human intelligence, signals intelligence, and imagery intelligence. All-source intelligence is used to analyze the risk of vulnerabilities (both intentional and unintentional) from development, manufacturing, and delivery processes, people, and the environment. The risk analysis may be performed on suppliers at multiple tiers in the supply chain sufficient to manage risks. Organizations may develop agreements to share all-source intelligence information or resulting decisions with other organizations, as appropriate.

Risk Assessment | Dynamic Threat Awareness (RA-3(3))

Description for Risk Assessment | Dynamic Threat Awareness (RA-3(3))
Determine the current cyber threat environment on an ongoing basis using [Assignment: organization-defined means].

Discussion for Risk Assessment | Dynamic Threat Awareness (RA-3(3))
The threat awareness information that is gathered feeds into the organization's information security operations to ensure that procedures are updated in response to the changing threat environment. For example, at higher threat levels, organizations may change the privilege or authentication thresholds required to perform certain operations.

Risk Assessment | Predictive Cyber Analytics (RA-3(4))

Description for Risk Assessment | Predictive Cyber Analytics (RA-3(4))
Employ the following advanced automation and analytics capabilities to predict and identify risks to [Assignment: organization-defined systems or system components]: [Assignment: organization-defined advanced automation and analytics capabilities].

Discussion for Risk Assessment | Predictive Cyber Analytics (RA-3(4))
A properly resourced Security Operations Center (SOC) or Computer Incident Response Team (CIRT) may be overwhelmed by the volume of information generated by the proliferation of security tools and appliances unless it employs advanced automation and analytics to analyze the data. Advanced automation and analytics capabilities are typically supported by artificial intelligence concepts, including machine learning. Examples include Automated Threat Discovery and Response (which includes broad-based collection, context-based analysis, and adaptive response capabilities), automated workflow operations, and machine assisted decision tools. Note, however, that sophisticated adversaries may be able to extract information related to analytic parameters and retrain the machine learning to classify malicious activity as benign. Accordingly, machine learning is augmented by human monitoring to ensure that sophisticated adversaries are not able to conceal their activities.

Risk Assessment Update (RA-4)

Description for Risk Assessment Update (RA-4)
[Withdrawn: Incorporated into RA-3.]

Discussion for Risk Assessment Update (RA-4)

Vulnerability Monitoring and Scanning (RA-5)

Description for Vulnerability Monitoring and Scanning (RA-5)
a. Monitor and scan for vulnerabilities in the system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system are identified and reported;
b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
1. Enumerating platforms, software flaws, and improper configurations;
2. Formatting checklists and test procedures; and
3. Measuring vulnerability impact;
c. Analyze vulnerability scan reports and results from vulnerability monitoring;
d. Remediate legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk;
e. Share information obtained from the vulnerability monitoring process and control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other systems; and
f. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.

Discussion for Vulnerability Monitoring and Scanning (RA-5)
Security categorization of information and systems guides the frequency and comprehensiveness of vulnerability monitoring (including scans). Organizations determine the required vulnerability monitoring for system components, ensuring that the potential sources of vulnerabilities—such as infrastructure components (e.g., switches, routers, guards, sensors), networked printers, scanners, and copiers—are not overlooked. The capability to readily update vulnerability monitoring tools as new vulnerabilities are discovered and announced and as new scanning methods are developed helps to ensure that new vulnerabilities are not missed by employed vulnerability monitoring tools. The vulnerability monitoring tool update process helps to ensure that potential vulnerabilities in the system are identified and addressed as quickly as possible. Vulnerability monitoring and analyses for custom software may require additional approaches, such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Organizations can use these analysis approaches in source code reviews and in a variety of tools, including web-based application scanners, static analysis tools, and binary analyzers.
Vulnerability monitoring includes scanning for patch levels; scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and scanning for flow control mechanisms that are improperly configured or operating incorrectly. Vulnerability monitoring may also include continuous vulnerability monitoring tools that use instrumentation to continuously analyze components. Instrumentation-based tools may improve accuracy and may be run throughout an organization without scanning. Vulnerability monitoring tools that facilitate interoperability include tools that are Security Content Automated Protocol (SCAP)-validated. Thus, organizations consider using scanning tools that

express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that employ the Open Vulnerability Assessment Language (OVAL) to determine the presence of vulnerabilities. Sources for vulnerability information include the Common Weakness Enumeration (CWE) listing and the National Vulnerability Database (NVD). Control assessments, such as red team exercises, provide additional sources of potential vulnerabilities for which to scan. Organizations also consider using scanning tools that express vulnerability impact by the Common Vulnerability Scoring System (CVSS).

Vulnerability monitoring includes a channel and process for receiving reports of security vulnerabilities from the public at-large. Vulnerability disclosure programs can be as simple as publishing a monitored email address or web form that can receive reports, including notification authorizing good-faith research and disclosure of security vulnerabilities. Organizations generally expect that such research is happening with or without their authorization and can use public vulnerability disclosure channels to increase the likelihood that discovered vulnerabilities are reported directly to the organization for remediation.

Organizations may also employ the use of financial incentives (also known as bug bounties) to further encourage external security researchers to report discovered vulnerabilities. Bug bounty programs can be tailored to the organization's needs. Bounties can be operated indefinitely or over a defined period of time and can be offered to the general public or to a curated group. Organizations may run public and private bounties simultaneously and could choose to offer partially credentialed access to certain participants in order to evaluate security vulnerabilities from privileged vantage points.

Vulnerability Monitoring and Scanning | Update Tool Capability (RA-5(1))

Description for Vulnerability Monitoring and Scanning | Update Tool Capability (RA-5(1))
[Withdrawn: Incorporated into RA-5.]

Discussion for Vulnerability Monitoring and Scanning | Update Tool Capability (RA-5(1))

Vulnerability Monitoring and Scanning | Update Vulnerabilities to Be Scanned (RA-5(2))

Description for Vulnerability Monitoring and Scanning | Update Vulnerabilities to Be Scanned (RA-5(2))
Update the system vulnerabilities to be scanned [Selection (one or more): [Assignment: organization-defined frequency]; prior to a new scan; when new vulnerabilities are identified and reported].

Discussion for Vulnerability Monitoring and Scanning | Update Vulnerabilities to Be Scanned (RA-5(2))
Due to the complexity of modern software, systems, and other factors, new vulnerabilities are discovered on a regular basis. It is important that newly discovered vulnerabilities are added to the list of vulnerabilities to be scanned to ensure that the organization can take steps to mitigate those vulnerabilities in a timely manner.

Vulnerability Monitoring and Scanning | Breadth and Depth of Coverage (RA-5(3))

Description for Vulnerability Monitoring and Scanning | Breadth and Depth of Coverage (RA-5(3))
Define the breadth and depth of vulnerability scanning coverage.

Discussion for Vulnerability Monitoring and Scanning | Breadth and Depth of Coverage (RA-5(3))
The breadth of vulnerability scanning coverage can be expressed as a percentage of components within the system, by the particular types of systems, by the criticality of systems, or by the number of vulnerabilities to be checked. Conversely, the depth of vulnerability scanning coverage can be expressed as the level of the system design that the organization intends to monitor (e.g., component, module, subsystem, element). Organizations can determine the sufficiency of vulnerability scanning coverage with regard to its risk tolerance and other factors. Scanning tools and how the tools are configured may affect the depth and coverage. Multiple scanning tools may be needed to achieve the desired depth and coverage. SP 800-53A provides additional information on the breadth and depth of coverage.

Vulnerability Monitoring and Scanning | Discoverable Information (RA-5(4))

Description for Vulnerability Monitoring and Scanning | Discoverable Information (RA-5(4))
Determine information about the system that is discoverable and take [Assignment: organization-defined corrective actions].

Discussion for Vulnerability Monitoring and Scanning | Discoverable Information (RA-5(4))
Discoverable information includes information that adversaries could obtain without compromising or breaching the system, such as by collecting information that the system is exposing or by conducting extensive web searches. Corrective actions include notifying appropriate organizational personnel, removing designated information, or changing the system to make the designated information less relevant or attractive to adversaries. This enhancement excludes intentionally discoverable information that may be part of a decoy capability (e.g., honeypots, honeynets, or deception nets) deployed by the organization.

Vulnerability Monitoring and Scanning | Privileged Access (RA-5(5))

Description for Vulnerability Monitoring and Scanning | Privileged Access (RA-5(5))
Implement privileged access authorization to [Assignment: organization-defined system components] for [Assignment: organization-defined vulnerability scanning activities].

Discussion for Vulnerability Monitoring and Scanning | Privileged Access (RA-5(5))
In certain situations, the nature of the vulnerability scanning may be more intrusive, or the system component that is the subject of the scanning may contain classified or controlled unclassified information, such as personally identifiable information. Privileged access authorization to selected system components facilitates more thorough vulnerability scanning and protects the sensitive nature of such scanning.

Vulnerability Monitoring and Scanning | Automated Trend Analyses (RA-5(6))

Description for Vulnerability Monitoring and Scanning | Automated Trend Analyses (RA-5(6))
Compare the results of multiple vulnerability scans using [Assignment: organization-defined automated mechanisms].

Discussion for Vulnerability Monitoring and Scanning | Automated Trend Analyses (RA-5(6))
Using automated mechanisms to analyze multiple vulnerability scans over time can help determine trends in system vulnerabilities and identify patterns of attack.

Vulnerability Monitoring and Scanning | Automated Detection and Notification of Unauthorized Components (RA-5(7))

Description for Vulnerability Monitoring and Scanning | Automated Detection and Notification of Unauthorized Components (RA-5(7))
[Withdrawn: Incorporated into CM-8.]

Discussion for Vulnerability Monitoring and Scanning | Automated Detection and Notification of Unauthorized Components (RA-5(7))

Vulnerability Monitoring and Scanning | Review Historic Audit Logs (RA-5(8))

Description for Vulnerability Monitoring and Scanning | Review Historic Audit Logs (RA-5(8))
Review historic audit logs to determine if a vulnerability identified in a [Assignment: organization-defined system] has been previously exploited within an [Assignment: organization-defined time period].

Discussion for Vulnerability Monitoring and Scanning | Review Historic Audit Logs (RA-5(8))
Reviewing historic audit logs to determine if a recently detected vulnerability in a system has been previously exploited by an adversary can provide important information for forensic analyses. Such analyses can help identify, for example, the extent of a previous intrusion, the trade craft employed during the attack, organizational information exfiltrated or modified, mission or business capabilities affected, and the duration of the attack.

Vulnerability Monitoring and Scanning | Penetration Testing and Analyses (RA-5(9))

Description for Vulnerability Monitoring and Scanning | Penetration Testing and Analyses (RA-5(9))
[Withdrawn: Incorporated into CA-8.]

Discussion for Vulnerability Monitoring and Scanning | Penetration Testing and Analyses (RA-5(9))

Vulnerability Monitoring and Scanning | Correlate Scanning Information (RA-5(10))

Description for Vulnerability Monitoring and Scanning | Correlate Scanning Information (RA-5(10))
Correlate the output from vulnerability scanning tools to determine the presence of multi-vulnerability and multi-hop attack vectors.

Discussion for Vulnerability Monitoring and Scanning | Correlate Scanning Information (RA-5(10))
An attack vector is a path or means by which an adversary can gain access to a system in order to deliver malicious code or exfiltrate information. Organizations can use attack trees to show how hostile activities by adversaries interact and combine to produce adverse impacts or negative consequences to systems and organizations. Such information, together with correlated data from vulnerability scanning tools, can provide greater clarity regarding multi-vulnerability and multi-hop attack vectors. The correlation of vulnerability scanning information is especially important when organizations are transitioning from older technologies to newer technologies (e.g., transitioning from IPv4 to IPv6 network protocols). During such transitions, some system components may inadvertently be unmanaged and create opportunities for adversary exploitation.

Vulnerability Monitoring and Scanning | Public Disclosure Program (RA-5(11))

Description for Vulnerability Monitoring and Scanning | Public Disclosure Program (RA-5(11))
Establish a public reporting channel for receiving reports of vulnerabilities in organizational systems and system components.

Discussion for Vulnerability Monitoring and Scanning | Public Disclosure Program (RA-5(11))
The reporting channel is publicly discoverable and contains clear language authorizing good-faith research and the disclosure of vulnerabilities to the organization. The organization does not condition its authorization on an expectation of indefinite non-disclosure to the public by the reporting entity but may request a specific time period to properly remediate the vulnerability.

Technical Surveillance Countermeasures Survey (RA-6)

Description for Technical Surveillance Countermeasures Survey (RA-6)
Employ a technical surveillance countermeasures survey at [Assignment: organization-defined locations] [Selection (one or more): [Assignment: organization-defined frequency]; when the following events or indicators occur: [Assignment: organization-defined events or indicators]].

Discussion for Technical Surveillance Countermeasures Survey (RA-6)
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 a 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.

Risk Response (RA-7)

Description for Risk Response (RA-7)
Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.

Discussion for Risk Response (RA-7)
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 that 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.

Privacy Impact Assessments (RA-8)

Description for Privacy Impact Assessments (RA-8)
Conduct privacy impact assessments for systems, programs, or other activities before:
a. Developing or procuring information technology that processes personally identifiable information; and
b. Initiating a new collection of personally identifiable information that:
1. Will be processed using information technology; and
2. Includes personally identifiable information permitting the physical or virtual (online) contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, ten or more individuals, other than agencies, instrumentalities, or employees of the federal government.

Discussion for Privacy Impact Assessments (RA-8)
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 analysis and a formal document that details the process and the outcome of the analysis.
Organizations conduct and develop a privacy impact assessment with sufficient clarity 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 senior agency official for privacy works closely with program managers, system owners, information technology experts, security officials, counsel, and other relevant organization personnel. Moreover, a privacy impact assessment is not a time-restricted activity that is limited to a particular milestone or stage of the information system or personally identifiable information life cycles. Rather, the privacy analysis continues throughout the system and personally identifiable information life cycles. Accordingly, a privacy impact assessment is a living document that organizations update whenever changes to the information technology, changes to the organization's practices, or other factors alter the privacy risks 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 that may have different names, 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 laws. 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.

Criticality Analysis (RA-9)

Description for Criticality Analysis (RA-9)
Identify critical system components and functions by performing a criticality analysis for [Assignment: organization-defined systems, system components, or system services] at [Assignment: organization-defined decision points in the system development life cycle].

Discussion for Criticality Analysis (RA-9)
Not all system components, functions, or services necessarily require significant protections. For example, criticality analysis is a key tenet of supply chain risk management and informs the prioritization of protection activities. The identification of critical system components and functions considers applicable laws, executive orders, regulations, directives, policies, standards, system functionality requirements, system and component interfaces, and system and component dependencies. Systems engineers 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 traceability 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 connections to and dependencies on cyber-physical systems, devices, system-of-systems, and outsourced IT services. System components that allow unmediated access to critical system components or functions are considered critical due to the inherent vulnerabilities that such components create. Component and function criticality are assessed in terms of the impact of a component or function failure on the organizational missions that are supported by the system that contains the components and functions.
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 life cycle, organizations may be able to modify the system design to reduce the critical nature of these components and functions, such as by adding redundancy or alternate 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 an important consideration. Such analysis is conducted as part of security categorization in RA-2.

Threat Hunting (RA-10)

Description for Threat Hunting (RA-10)
a. Establish and maintain a cyber threat hunting capability to:
1. Search for indicators of compromise in organizational systems; and
2. Detect, track, and disrupt threats that evade existing controls; and
b. Employ the threat hunting capability [Assignment: organization-defined frequency].

Discussion for Threat Hunting (RA-10)
Threat hunting is an active means of cyber defense in contrast to traditional protection measures, such as firewalls, intrusion detection and prevention systems, quarantining malicious code in sandboxes, and Security Information 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 teams leverage existing threat intelligence and 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.

Policy and Procedures (SA-1)

Description for Policy and Procedures (SA-1)
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] system and services acquisition policy that:
(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the system and services acquisition policy and the associated system and services acquisition controls;
b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and services acquisition policy and procedures; and
c. Review and update the current system and services acquisition:
1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

Discussion for Policy and Procedures (SA-1)
System and services acquisition policy and procedures address the controls in the SA family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of system and services acquisition policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, 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. Events that may precipitate an update to system and services acquisition policy and procedures include assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Allocation of Resources (SA-2)

Description for Allocation of Resources (SA-2)
a. Determine the high-level information security and privacy requirements for the system or system service in mission and business process planning;
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.

Discussion for Allocation of Resources (SA-2)
Resource allocation for information security and privacy includes funding for system and services acquisition, sustainment, and supply chain-related risks throughout the system development life cycle.

System Development Life Cycle (SA-3)

Description for System Development Life Cycle (SA-3)
a. Acquire, develop, and manage the system using [Assignment: organization-defined system development life cycle] that incorporates information security and privacy considerations;
b. Define and document information security and privacy roles and responsibilities throughout the system development life cycle;
c. Identify individuals having information security and privacy roles and responsibilities; and
d. Integrate the organizational information security and privacy risk management process into system development life cycle activities.

Discussion for System Development Life Cycle (SA-3)
A system development life cycle process provides the foundation for the successful development, implementation, and operation of organizational systems. The integration of security and privacy considerations early in the system development life cycle is a foundational principle of systems security engineering and privacy engineering. To apply the required controls within the system development life cycle requires a basic understanding of information security and privacy, threats, vulnerabilities, adverse impacts, and risk to critical mission and business functions. The security engineering principles in SA-8 help individuals properly design, code, and test systems and system components. Organizations include qualified personnel (e.g., senior agency information security officers, senior agency officials for privacy, security and privacy architects, and security and privacy engineers) in system development life cycle processes to ensure that established security and privacy requirements are incorporated into organizational systems. Role-based security and privacy training programs can ensure that individuals with key security and privacy roles and responsibilities have the experience, skills, and expertise to conduct assigned system development life cycle activities.
The effective integration of security and privacy requirements into enterprise architecture also helps to ensure that important security and privacy considerations are addressed throughout the system life cycle and that those considerations are directly related to organizational mission and business processes. This process also facilitates the integration of the information security and privacy architectures into the enterprise architecture, consistent with the risk management strategy of the organization. Because the system development life cycle involves multiple organizations, (e.g., external suppliers, developers, integrators, service providers), acquisition and supply chain risk management functions and controls play significant roles in the effective management of the system during the life cycle.

System Development Life Cycle | Manage Preproduction Environment (SA-3(1))

Description for System Development Life Cycle | Manage Preproduction Environment (SA-3(1))
Protect system preproduction environments commensurate with risk throughout the system development life cycle for the system, system component, or system service.

Discussion for System Development Life Cycle | Manage Preproduction Environment (SA-3(1))
The preproduction environment includes development, test, and integration environments. The program protection planning processes established by the Department of Defense are examples 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.

System Development Life Cycle | Use of Live or Operational Data (SA-3(2))

Description for System Development Life Cycle | Use of Live or Operational Data (SA-3(2))
(a) Approve, 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 in use within the preproduction environments.

Discussion for System Development Life Cycle | Use of Live or Operational Data (SA-3(2))
Live data is also referred to as operational data. The use of live or operational data in preproduction (i.e., development, test, and integration) environments can result in significant risks to organizations. In addition, the use of personally identifiable information in testing, research, and training increases the risk of unauthorized disclosure or misuse of such information. Therefore, it is important for the organization to manage any additional risks that may result from the use of live or operational data. Organizations can minimize such risks by using test or dummy data 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.

System Development Life Cycle | Technology Refresh (SA-3(3))

Description for System Development Life Cycle | Technology Refresh (SA-3(3))
Plan for and implement a technology refresh schedule for the system throughout the system development life cycle.

Discussion for System Development Life Cycle | Technology Refresh (SA-3(3))
Technology refresh planning may encompass hardware, software, firmware, processes, personnel skill sets, suppliers, service providers, and facilities. The use of obsolete or nearing obsolete technology may increase the security and privacy risks associated with unsupported components, counterfeit or repurposed components, components unable to implement security or privacy requirements, slow or inoperable components, components from untrusted sources, inadvertent personnel error, or increased complexity. Technology refreshes typically occur during the operations and maintenance stage of the system development life cycle.

Acquisition Process (SA-4)

Description for Acquisition Process (SA-4)
Include the following requirements, descriptions, and criteria, explicitly or by reference, using [Selection (one or more): standardized contract language; [Assignment: organization-defined contract language]] in the acquisition contract for the system, system component, or system service:
a. Security and privacy functional requirements;
b. Strength of mechanism requirements;
c. Security and privacy assurance requirements;
d. Controls needed to satisfy the security and privacy requirements.
e. Security and privacy documentation requirements;
f. Requirements for protecting security and privacy documentation;
g. Description of the system development environment and environment in which the system is intended to operate;
h. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; and
i. Acceptance criteria.

Discussion for Acquisition Process (SA-4)
Security and privacy functional requirements are typically derived from the high-level security and privacy requirements described in SA-2. The derived requirements include security and privacy capabilities, functions, and mechanisms. Strength requirements associated with such capabilities, functions, and mechanisms include degree of correctness, completeness, resistance to tampering or bypass, and resistance to direct attack. Assurance requirements include development processes, procedures, and methodologies as well as the evidence from development and assessment activities that provide grounds for confidence that the required functionality is implemented and possesses the required strength of mechanism. SP 800-160-1 describes the process of requirements engineering as part of the system development life cycle.
Controls can be viewed as descriptions of the safeguards and protection capabilities appropriate for achieving the particular security and privacy objectives of the organization and for reflecting 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, administrative, and physical aspects. In some cases, the selection and implementation of a control may necessitate additional specification by the organization in the form of derived requirements or instantiated 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 address all stages of the system development life cycle. Documentation provides user and administrator guidance

for the implementation and operation of controls. The level of detail required in such documentation is based on the security categorization or classification level of the system and the degree to which organizations depend on the capabilities, functions, or mechanisms to meet risk response expectations. Requirements can include mandated configuration settings that specify allowed functions, ports, protocols, and services. Acceptance criteria for systems, system components, and system services are defined in the same manner as the criteria for any organizational acquisition or procurement.

Acquisition Process | Functional Properties of Controls (SA-4(1))

Description for Acquisition Process | Functional Properties of Controls (SA-4(1))
Require the developer of the system, system component, or system service to provide a description of the functional properties of the controls to be implemented.

Discussion for Acquisition Process | Functional Properties of Controls (SA-4(1))
Functional properties of security and privacy controls describe the functionality (i.e., security or privacy capability, functions, or mechanisms) visible at the interfaces of the controls and specifically exclude functionality and data structures internal to the operation of the controls.

Acquisition Process | Design and Implementation Information for Controls (SA-4(2))

Description for Acquisition Process | Design and Implementation Information for Controls (SA-4(2))
Require the developer of the system, system component, or system service to provide design and implementation information for the controls that includes: [Selection (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; [Assignment: organization-defined design and implementation information]] at [Assignment: organization-defined level of detail].

Discussion for Acquisition Process | Design and Implementation Information for Controls (SA-4(2))
Organizations may require different levels of detail in the documentation for the design and implementation of controls in organizational systems, system components, or system services based on mission and business requirements, requirements for resiliency and trustworthiness, and requirements for analysis and testing. Systems can be partitioned into multiple subsystems. Each subsystem within the system can contain one or more modules. The high-level design for the system is expressed in terms of subsystems and the interfaces between subsystems providing security-relevant functionality. The low-level design for the system is expressed in terms of modules and the interfaces between modules providing security-relevant functionality. Design and implementation documentation can include manufacturer, version, serial number, verification hash signature, software libraries used, date of purchase or download, and the vendor or download source. Source code and hardware schematics are referred to as the implementation representation of the system.

Acquisition Process | Development Methods, Techniques, and Practices (SA-4(3))

Description for Acquisition Process | Development Methods, Techniques, and Practices (SA-4(3))
Require the developer of the system, system component, or system service to demonstrate the use of a system development life cycle process that includes:
(a) [Assignment: organization-defined systems engineering methods];
(b) <assign:#>organization-defined [Selection (one or more): systems security; privacy<#:assign> engineering methods]; and
(c) [Assignment: organization-defined software development methods; testing, evaluation, assessment, verification, and validation methods; and quality control processes].

Discussion for Acquisition Process | Development Methods, Techniques, and Practices (SA-4(3))
Following a system development life cycle that includes state-of-the-practice software development methods, systems engineering methods, systems security and privacy engineering methods, and quality control processes helps to reduce the number and severity of latent errors within systems, system components, and system services. Reducing the number and severity of such errors reduces the number of vulnerabilities in those systems, components, and services. Transparency in the methods and techniques that developers select and implement for systems engineering, systems security and privacy engineering, software development, component and system assessments, and quality control processes provides an increased level of assurance in the trustworthiness of the system, system component, or system service being acquired.

Supply Chain Protection (SA-12)

Description for Supply Chain Protection (SA-12)
[Withdrawn: Incorporated into SR Family.]

Discussion for Supply Chain Protection (SA-12)

Acquisition Process | System, Component, and Service Configurations (SA-4(5))

Description for Acquisition Process | System, Component, and Service Configurations (SA-4(5))
Require the developer of the system, system component, or system service to:
(a) Deliver the system, component, or service with [Assignment: organization-defined security configurations] implemented; and
(b) Use the configurations as the default for any subsequent system, component, or service reinstallation or upgrade.

Discussion for Acquisition Process | System, Component, and Service Configurations (SA-4(5))
Examples of security configurations include the U.S. Government Configuration Baseline (USGCB), Security Technical Implementation Guides (STIGs), and any limitations on functions, ports, protocols, and services. Security characteristics can include requiring that default passwords have been changed.

Acquisition Process | Use of Information Assurance Products (SA-4(6))

Description for Acquisition Process | Use of Information Assurance Products (SA-4(6))
(a) Employ only government off-the-shelf or commercial off-the-shelf information assurance and information assurance-enabled information technology products that compose an NSA-approved solution to protect classified information when the networks used to transmit the information are at a lower classification level than the information being transmitted; and
(b) Ensure that these products have been evaluated and/or validated by NSA or in accordance with NSA-approved procedures.

Discussion for Acquisition Process | Use of Information Assurance Products (SA-4(6))
Commercial off-the-shelf IA or IA-enabled information technology products used to protect classified information by cryptographic means may be required to use NSA-approved key management. See NSA CSFC.

Acquisition Process | NIAP-approved Protection Profiles (SA-4(7))

Description for Acquisition Process | NIAP-approved Protection Profiles (SA-4(7))
(a) Limit the use of commercially provided information assurance and information assurance-enabled information technology products to those products that have been successfully evaluated against a National Information Assurance partnership (NIAP)-approved Protection Profile for a specific technology type, if such a profile exists; and
(b) Require, if no NIAP-approved Protection Profile exists for a specific technology type but a commercially provided information technology product relies on cryptographic functionality to enforce its security policy, that the cryptographic module is FIPS-validated or NSA-approved.

Discussion for Acquisition Process | NIAP-approved Protection Profiles (SA-4(7))
See NIAP CCEVS for additional information on NIAP. See NIST CMVP for additional information on FIPS-validated cryptographic modules.

Acquisition Process | Continuous Monitoring Plan for Controls (SA-4(8))

Description for Acquisition Process | Continuous Monitoring Plan for Controls (SA-4(8))
Require the developer of the system, system component, or system service to produce a plan for continuous monitoring of control effectiveness that is consistent with the continuous monitoring program of the organization.

Discussion for Acquisition Process | Continuous Monitoring Plan for Controls (SA-4(8))
The objective of continuous monitoring plans is to determine if the planned, required, and deployed controls within the system, system component, or system service continue to be effective over time based on the inevitable changes that occur. Developer continuous monitoring plans include a sufficient level of detail such that the information can be incorporated into continuous monitoring programs implemented by organizations. Continuous monitoring plans can include the types of control assessment and monitoring activities planned, frequency of control monitoring, and actions to be taken when controls fail or become ineffective.

Acquisition Process | Functions, Ports, Protocols, and Services in Use (SA-4(9))

Description for Acquisition Process | Functions, Ports, Protocols, and Services in Use (SA-4(9))
Require the developer of the system, system component, or system service to identify the functions, ports, protocols, and services intended for organizational use.

Discussion for Acquisition Process | Functions, Ports, Protocols, and Services in Use (SA-4(9))
The identification of functions, ports, protocols, and services early in the system development life cycle (e.g., 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 development 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 requiring system service providers to do so. Early identification of functions, ports, protocols, and services avoids costly retrofitting of controls after the 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.

Acquisition Process | Use of Approved PIV Products (SA-4(10))

Description for Acquisition Process | Use of Approved PIV Products (SA-4(10))
Employ only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational systems.

Discussion for Acquisition Process | Use of Approved PIV Products (SA-4(10))
Products on the FIPS 201-approved products list meet NIST requirements for Personal Identity Verification (PIV) of Federal Employees and Contractors. PIV cards are used for multi-factor authentication in systems and organizations.

Acquisition Process | System of Records (SA-4(11))

Description for Acquisition Process | System of Records (SA-4(11))
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.

Discussion for Acquisition Process | System of Records (SA-4(11))
When, by contract, an organization provides for the operation of a system of records to accomplish an organizational mission or function, the organization, consistent with its authority, causes the requirements of the PRIVACT to be applied to the system of records.

Acquisition Process | Data Ownership (SA-4(12))

Description for Acquisition Process | Data Ownership (SA-4(12))
(a) Include organizational data ownership requirements in the acquisition contract; and
(b) Require all data to be removed from the contractor's system and returned to the organization within [Assignment: organization-defined time frame].

Discussion for Acquisition Process | Data Ownership (SA-4(12))
Contractors who operate a system that contains data owned by an organization initiating the contract have policies and procedures in place to remove the data from their systems and/or return the data in a time frame defined by the contract.

System Documentation (SA-5)

Description for System Documentation (SA-5)
a. Obtain or develop administrator documentation for the system, system component, or system service that describes:
1. Secure configuration, installation, and operation of the system, component, or service;
2. Effective use and maintenance of security and privacy functions and mechanisms; and
3. Known vulnerabilities regarding configuration and use of administrative or privileged functions;
b. Obtain or develop user documentation for the system, system component, or system service that describes:
1. User-accessible security and privacy functions and mechanisms and how to effectively use those functions and mechanisms;
2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner and protect individual privacy; and
3. User responsibilities in maintaining the security of the system, component, or service and privacy of individuals;
c. Document attempts to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent and take [Assignment: organization-defined actions] in response; and
d. Distribute documentation to [Assignment: organization-defined personnel or roles].

Discussion for System Documentation (SA-5)
System documentation helps personnel understand the implementation and operation of controls. Organizations consider establishing specific measures to determine the quality and completeness of the content provided. System

documentation may be used to support the management of supply chain risk, incident response, and other functions. Personnel or roles that require documentation include system owners, system security officers, and system administrators. Attempts to obtain documentation include contacting manufacturers or suppliers and conducting web-based searches. The inability to obtain documentation may occur due to the age of the system or component or the lack of support from developers and contractors. When documentation cannot be obtained, organizations may need to recreate the documentation if it is essential to the implementation or operation of the controls. The protection provided for the documentation is commensurate with the security category or classification of the system. Documentation that addresses system vulnerabilities may require an increased level of protection. Secure operation of the system includes initially starting the system and resuming secure system operation after a lapse in system operation.

Supply Chain Protection | Acquisition Strategies / Tools / Methods (SA-12(1))

Description for Supply Chain Protection | Acquisition Strategies / Tools / Methods (SA-12(1))
[Withdrawn: Moved to SR-5.]

Discussion for Supply Chain Protection | Acquisition Strategies / Tools / Methods (SA-12(1))

Supply Chain Protection | Validate as Genuine and Not Altered (SA-12(10))

Description for Supply Chain Protection | Validate as Genuine and Not Altered (SA-12(10))
[Withdrawn: Moved to SR-4(3).]

Discussion for Supply Chain Protection | Validate as Genuine and Not Altered (SA-12(10))

Supply Chain Protection | Penetration Testing / Analysis of Elements, Processes, and Actors (SA-12(11))

Description for Supply Chain Protection | Penetration Testing / Analysis of Elements, Processes, and Actors (SA-12(11))
[Withdrawn: Moved to SR-6(1).]

Discussion for Supply Chain Protection | Penetration Testing / Analysis of Elements, Processes, and Actors (SA-12(11))

Supply Chain Protection | Inter-organizational Agreements (SA-12(12))

Description for Supply Chain Protection | Inter-organizational Agreements (SA-12(12))
[Withdrawn: Moved to SR-8.]

Discussion for Supply Chain Protection | Inter-organizational Agreements (SA-12(12))

Supply Chain Protection | Critical Information System Components (SA-12(13))

Description for Supply Chain Protection | Critical Information System Components (SA-12(13))
[Withdrawn: Incorporated into MA-6 and RA-9.]

Discussion for Supply Chain Protection | Critical Information System Components (SA-12(13))

Supply Chain Protection | Identity and Traceability (SA-12(14))

Description for Supply Chain Protection | Identity and Traceability (SA-12(14))
[Withdrawn: Moved to SR-4(1) and SR-4(2).]

Discussion for Supply Chain Protection | Identity and Traceability (SA-12(14))

Supply Chain Protection | Processes to Address Weaknesses or Deficiencies (SA-12(15))

Description for Supply Chain Protection | Processes to Address Weaknesses or Deficiencies (SA-12(15))
[Withdrawn: Incorporated into SR-3.]

Discussion for Supply Chain Protection | Processes to Address Weaknesses or Deficiencies (SA-12(15))

Security and Privacy Engineering Principles (SA-8)

Description for Security and Privacy Engineering Principles (SA-8)
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].

Discussion for Security and Privacy Engineering Principles (SA-8)
Systems security and privacy engineering principles are closely related to and implemented throughout the system development life cycle (see SA-3). 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 reduces the susceptibility to disruptions, hazards, threats, and the creation of privacy problems for individuals. Examples of system 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; delineating physical and logical security boundaries; ensuring that developers are trained on how to build secure software; tailoring controls to meet organizational needs; and 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 system 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 incorporating tamper-resistant hardware into a design.

Security and Privacy Engineering Principles | Clear Abstractions (SA-8(1))

Description for Security and Privacy Engineering Principles | Clear Abstractions (SA-8(1))
Implement the security design principle of clear abstractions.

Discussion for Security and Privacy Engineering Principles | Clear Abstractions (SA-8(1))
The principle of clear abstractions states that a system has simple, well-defined interfaces and functions that provide a consistent and intuitive view of the data and how the data is managed. The clarity, simplicity, necessity, and sufficiency of the system interfaces— combined with a precise definition of their functional behavior—promotes ease of analysis, inspection, and testing as well as the correct and secure use of the system. The clarity of an abstraction is subjective. Examples that reflect the application of this principle include avoidance of redundant, unused interfaces; information hiding; and avoidance of semantic overloading of interfaces or their parameters. Information hiding (i.e., representation-independent programming), is a design discipline used to ensure that the internal representation of information in one system component is not visible to another system component invoking or calling the first component, such that the published abstraction is not influenced by how the data may be managed internally.

Security and Privacy Engineering Principles | Least Common Mechanism (SA-8(2))

Description for Security and Privacy Engineering Principles | Least Common Mechanism (SA-8(2))
Implement the security design principle of least common mechanism in [Assignment: organization-defined systems or system components].

Discussion for Security and Privacy Engineering Principles | Least Common Mechanism (SA-8(2))
The principle of least common mechanism states that the amount of mechanism common to more than one user and depended on by all users is minimized POPEK74. Mechanism minimization implies that different components of a system refrain from using the same mechanism to access a system resource. Every shared mechanism (especially a mechanism involving shared variables) represents a potential information path between users and is designed with care to ensure that it does not unintentionally compromise security SALTZER75. Implementing the principle of least common mechanism helps to reduce the adverse consequences of sharing the system state among different programs. A single program that corrupts 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 LAMPSON73.

Security and Privacy Engineering Principles | Modularity and Layering (SA-8(3))

Description for Security and Privacy Engineering Principles | Modularity and Layering (SA-8(3))
Implement the security design principles of modularity and layering in [Assignment: organization-defined systems or system components].

Discussion for Security and Privacy Engineering Principles | Modularity and Layering (SA-8(3))
The principles of modularity and layering are fundamental across system engineering disciplines. Modularity and layering derived from functional decomposition are effective in managing system complexity by making it possible to comprehend the structure of the system. Modular decomposition, or refinement in system design, is challenging and resists general statements of principle. Modularity serves to isolate functions and related data structures into well-defined logical units. Layering allows the relationships of these units to be better understood so that dependencies are clear and undesired complexity can be avoided. The security design principle of modularity extends functional modularity to include considerations based on trust, trustworthiness, privilege, and security policy. Security-informed modular decomposition includes the allocation of policies to systems in a network, separation of system applications into processes with distinct address spaces, allocation of system policies to layers, and separation of processes into subjects with distinct privileges based on hardware-supported privilege domains.

Security and Privacy Engineering Principles | Partially Ordered Dependencies (SA-8(4))

Description for Security and Privacy Engineering Principles | Partially Ordered Dependencies (SA-8(4))
Implement the security design principle of partially ordered dependencies in [Assignment: organization-defined systems or system components].

Discussion for Security and Privacy Engineering Principles | Partially Ordered Dependencies (SA-8(4))
The principle of partially ordered dependencies states that the synchronization, calling, and other dependencies in the system are partially ordered. A fundamental concept in system design is layering, whereby the system is organized into well-defined, functionally related modules or components. The layers are linearly ordered with respect to inter-layer dependencies, such that higher layers are dependent on lower layers. While providing functionality to higher layers, some layers can be self-contained and not dependent on lower layers. While a partial ordering of all functions in a given system may not be possible, if circular dependencies are constrained to occur within layers, the inherent problems of circularity can be more easily managed. Partially ordered dependencies and system layering contribute significantly to the simplicity and coherency of the system design. Partially ordered dependencies also facilitate system testing and analysis.

Security and Privacy Engineering Principles | Efficiently Mediated Access (SA-8(5))

Description for Security and Privacy Engineering Principles | Efficiently Mediated Access (SA-8(5))
Implement the security design principle of efficiently mediated access in [Assignment: organization-defined systems or system components].

Discussion for Security and Privacy Engineering Principles | Efficiently Mediated Access (SA-8(5))
The principle of efficiently mediated access states that policy enforcement mechanisms utilize the least common mechanism available while satisfying stakeholder requirements within expressed constraints. The mediation of access to system resources (i.e., CPU, memory, devices, communication ports, services, infrastructure, data, and information) is often the predominant security function of secure systems. It also enables the realization of protections for the capability provided to stakeholders by the system. Mediation of resource access can result in performance bottlenecks if the system is not designed correctly. For example, by using hardware mechanisms, efficiently mediated access can be achieved. Once access to a low-level resource such as memory has been obtained, hardware protection mechanisms can ensure that out-of-bounds access does not occur.

Security and Privacy Engineering Principles | Minimized Sharing (SA-8(6))

Description for Security and Privacy Engineering Principles | Minimized Sharing (SA-8(6))
Implement the security design principle of minimized sharing in [Assignment: organization-defined systems or system components].

Discussion for Security and Privacy Engineering Principles | Minimized Sharing (SA-8(6))
The principle of minimized sharing states that no computer resource is shared between system components (e.g., subjects, processes, functions) unless it is absolutely necessary to do so. Minimized sharing helps to simplify system design and implementation. In order to protect user-domain resources from arbitrary active entities, no resource is shared unless that sharing has been explicitly requested and granted. The need for resource sharing can be motivated by the design principle of least common mechanism in the case of internal entities or driven by stakeholder requirements. However, internal sharing is carefully designed to avoid performance and covert storage and timing channel problems. Sharing via common mechanism can increase the susceptibility of data and information to unauthorized access, disclosure, use, or modification and can adversely affect the inherent capability provided by the system. To minimize sharing induced by common mechanisms, such mechanisms can be designed to be reentrant or virtualized to preserve separation. Moreover, the use of global data to share information is carefully scrutinized. The lack of encapsulation may obfuscate relationships among the sharing entities.

Security and Privacy Engineering Principles | Reduced Complexity (SA-8(7))

Description for Security and Privacy Engineering Principles | Reduced Complexity (SA-8(7))
Implement the security design principle of reduced complexity in [Assignment: organization-defined systems or system components].

Discussion for Security and Privacy Engineering Principles | Reduced Complexity (SA-8(7))
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 analyzable, 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 analyses performed to obtain evidence about the emergent security property of the system. For such analyses 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 the 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; that is, simpler systems contain fewer vulnerabilities. An benefit of reduced complexity is that it is easier to understand whether the intended 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 any such conclusion about correctness, completeness, and the existence of vulnerabilities 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.

Security and Privacy Engineering Principles | Secure Evolvability (SA-8(8))

Description for Security and Privacy Engineering Principles | Secure Evolvability (SA-8(8))
Implement the security design principle of secure evolvability in [Assignment: organization-defined systems or system components].

Discussion for Security and Privacy Engineering Principles | Secure Evolvability (SA-8(8))
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, interconnections (i.e., system architecture), functionality, or configuration (i.e., security policy enforcement). Changes include a new, enhanced, or 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 direction, 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 trustworthiness 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-methodical manner. The benefits of this principle include reduced vendor life cycle costs, reduced cost of ownership, improved system security, more effective management of security risk, and less risk uncertainty.

Security and Privacy Engineering Principles | Trusted Components (SA-8(9))

Description for Security and Privacy Engineering Principles | Trusted Components (SA-8(9))
Implement the security design principle of trusted components in [Assignment: organization-defined systems or system components].

Discussion for Security and Privacy Engineering Principles | Trusted Components (SA-8(9))
The principle of trusted components states that a component is trustworthy to at least a level 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 the trust is not consequently misplaced. Ultimately, this principle demands some metric by which the trust in 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 subsystem), which may have varying levels of trustworthiness. The conservative assumption is that the trustworthiness of a compound component is that of its least trustworthy subcomponent. 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, any such rationale reflects logical reasoning based on a clear statement of the trustworthiness objectives as well as relevant and credible evidence. The trustworthiness of a compound component is not the same as increased application of defense-in-depth layering within the component or a replication of components. Defense-in-depth techniques do not increase the trustworthiness of the whole above that of the least trustworthy component.

Security and Privacy Engineering Principles | Hierarchical Trust (SA-8(10))

Description for Security and Privacy Engineering Principles | Hierarchical Trust (SA-8(10))
Implement the security design principle of hierarchical trust in [Assignment: organization-defined systems or system components].

Discussion for Security and Privacy Engineering Principles | Hierarchical Trust (SA-8(10))
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 an assurance case (assurance argument) when composing a secure system from heterogeneously trustworthy components. To analyze a system composed of heterogeneously trustworthy components for its trustworthiness, it is essential to eliminate circular dependencies with regard to the trustworthiness. If a more trustworthy component located in a lower layer of the system were to depend on a less trustworthy component in a higher layer, this would, in effect, put the components in the same less trustworthy equivalence class per the principle of trusted components. Trust relationships, or chains of trust, can have various manifestations. 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 trustworthy nodes. Another example occurs in a layered high-assurance system where the security kernel (including the hardware base), 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 overly 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.

Security and Privacy Engineering Principles | Inverse Modification Threshold (SA-8(11))

Description for Security and Privacy Engineering Principles | Inverse Modification Threshold (SA-8(11))
Implement the security design principle of inverse modification threshold in [Assignment: organization-defined systems or system components].

Discussion for Security and Privacy Engineering Principles | Inverse Modification Threshold (SA-8(11))
The principle of inverse modification threshold builds on the principle of trusted components and the principle of hierarchical trust and states that the degree of protection provided to a component is commensurate with its trustworthiness. As the trust placed in a component increases, the protection against unauthorized modification of the component also increases to the same degree. Protection from unauthorized modification can come in the form of the component's own self-protection and innate trustworthiness, or it can come from the protections afforded to the component from other elements or attributes of the security architecture (to include protections in the environment of operation).

Security and Privacy Engineering Principles | Hierarchical Protection (SA-8(12))

Description for Security and Privacy Engineering Principles | Hierarchical Protection (SA-8(12))
Implement the security design principle of hierarchical protection in [Assignment: organization-defined systems or system components].

Discussion for Security and Privacy Engineering Principles | Hierarchical Protection (SA-8(12))
The principle of hierarchical protection states that a component need not be protected from more trustworthy components. In the degenerate case of the most trusted 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 untrusted applications it supports, but the applications, conversely, do not need to protect themselves from the kernel. The trustworthiness of users 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 system high environments where users are highly trustworthy and where other protections are put in place to bound and protect the system high execution environment.

Security and Privacy Engineering Principles | Minimized Security Elements (SA-8(13))

Description for Security and Privacy Engineering Principles | Minimized Security Elements (SA-8(13))
Implement the security design principle of minimized security elements in [Assignment: organization-defined systems or system components].

Discussion for Security and Privacy Engineering Principles | Minimized Security Elements (SA-8(13))
The principle of minimized security elements states that the system does not have extraneous trusted 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 costlier to construct and implement, owing to the increased rigor of development processes. Trusted components require greater security analysis to qualify their trustworthiness. 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 ascertain 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.

Security and Privacy Engineering Principles | Least Privilege (SA-8(14))

Description for Security and Privacy Engineering Principles | Least Privilege (SA-8(14))
Implement the security design principle of least privilege in [Assignment: organization-defined systems or system components].

Discussion for Security and Privacy Engineering Principles | Least Privilege (SA-8(14))
The principle of least privilege states that each system component is allocated sufficient privileges to accomplish its specified functions 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. Interfaces used to invoke component capability are available to only certain subsets of the user population, and component design supports a sufficiently fine granularity of privilege decomposition. For example, in the case of an audit mechanism, there may be an interface for the audit manager, who configures the audit settings; an interface for the audit operator, who ensures that audit data is safely collected and stored; and, finally, yet another interface for the audit reviewer, who only has need to view the audit data that has been collected but no need to perform operations on that data. In addition to its manifestations at the system interface, least privilege can be used as a guiding principle for the internal structure of the system itself. One aspect of internal least privilege is to construct modules so that only the elements encapsulated by the module are directly operated on by the functions 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 internal 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 for the elements (e.g., read, write) are minimal.

Security and Privacy Engineering Principles | Predicate Permission (SA-8(15))

Description for Security and Privacy Engineering Principles | Predicate Permission (SA-8(15))
Implement the security design principle of predicate permission in [Assignment: organization-defined systems or system components].

Discussion for Security and Privacy Engineering Principles | Predicate Permission (SA-8(15))
The principle of predicate permission states that system designers consider requiring multiple authorized entities to provide consent before a highly critical operation or access to highly sensitive data, information, or resources is allowed to proceed. SALTZER75 originally named predicate permission the separation of privilege. It is also equivalent to separation of duty. The division of privilege among multiple parties decreases the likelihood of abuse and provides the safeguard that no single accident, deception, or breach of trust is sufficient to enable an unrecoverable action that can lead to significantly damaging effects. The design options for such a mechanism may require simultaneous action (e.g., the firing of a nuclear weapon requires two different authorized individuals to give the correct command within a small time window) or a sequence of operations where each successive action is enabled by some prior action, but no single individual is able to enable more than one action.

Security and Privacy Engineering Principles | Self-reliant Trustworthiness (SA-8(16))

Description for Security and Privacy Engineering Principles | Self-reliant Trustworthiness (SA-8(16))
Implement the security design principle of self-reliant trustworthiness in [Assignment: organization-defined systems or system components].

Discussion for Security and Privacy Engineering Principles | Self-reliant Trustworthiness (SA-8(16))
The principle of self-reliant trustworthiness states that systems minimize their reliance on other systems for their own trustworthiness. A system is trustworthy by default, and any connection to an external entity is used to supplement its function. If a system were required to maintain a connection with another external entity in order to maintain its trustworthiness, then that system would be vulnerable to malicious and non-malicious threats that could result in the loss or degradation of that connection. The benefit of the principle of self-reliant trustworthiness is that the isolation of a system will make it less vulnerable to attack. A corollary to this principle relates to the ability of the system (or system component) to operate in isolation and then resynchronize with other components when it is rejoined with them.

Security and Privacy Engineering Principles | Secure Distributed Composition (SA-8(17))

Description for Security and Privacy Engineering Principles | Secure Distributed Composition (SA-8(17))
Implement the security design principle of secure distributed composition in [Assignment: organization-defined systems or system components].

Discussion for Security and Privacy Engineering Principles | Secure Distributed Composition (SA-8(17))
The principle of secure distributed composition states that the composition of distributed components that enforce the same system security policy result 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 a capability from the composition of distributed components can magnify the relevancy of these principles. In particular, the translation of security policy from a stand-alone 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.

Security and Privacy Engineering Principles | Trusted Communications Channels (SA-8(18))

Description for Security and Privacy Engineering Principles | Trusted Communications Channels (SA-8(18))
Implement the security design principle of trusted communications channels in [Assignment: organization-defined systems or system components].

Discussion for Security and Privacy Engineering Principles | Trusted Communications Channels (SA-8(18))
The principle of trusted communication channels states that when composing a system where there 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 and modification and to further increase the assurance of proper end-to-end communication).

Security and Privacy Engineering Principles | Continuous Protection (SA-8(19))

Description for Security and Privacy Engineering Principles | Continuous Protection (SA-8(19))
Implement the security design principle of continuous protection in [Assignment: organization-defined systems or system components].

Discussion for Security and Privacy Engineering Principles | Continuous Protection (SA-8(19))
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 assurances 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 delivered capability require that data and information are continuously protected. That is, there are no periods during which data and information are left unprotected while under control of the system (i.e., during the creation, storage, processing, or communication of the data and information, as well as during system initialization, execution, failure, interruption, and shutdown). Continuous protection requires adherence to the precepts of the reference monitor concept (i.e., every request is validated by the reference monitor; the reference monitor is able to 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 alternative operational modes).
Continuous protection also applies to systems designed to operate in varying configurations, 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 need that drives 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 verification 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 atomic and that any residual effects from the old policy are guaranteed to not conflict with the new policy. The ability to demonstrate continuous protection is rooted in the clear articulation of life cycle protection needs as stakeholder security requirements.

Security and Privacy Engineering Principles | Secure Metadata Management (SA-8(20))

Description for Security and Privacy Engineering Principles | Secure Metadata Management (SA-8(20))
Implement the security design principle of secure metadata management in [Assignment: organization-defined systems or system components].

Discussion for Security and Privacy Engineering Principles | Secure Metadata Management (SA-8(20))
The principle of secure metadata management states that metadata are first class objects with respect to security policy when the policy requires either complete protection of information or that the security subsystem be self-protecting. The principle of secure metadata management is driven by the recognition that a system, subsystem, or component cannot achieve self-protection unless it protects the data it relies on for correct execution. Data is generally not interpreted by the system that stores it. It may have semantic value (i.e., it comprises 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 classification level or impact level of a file name), including self-referential metadata.
The apparent secondary nature of metadata can lead to neglect of its legitimate need for protection, resulting in a violation of the security policy that includes the exfiltration of information. A particular concern associated with insufficient protections for metadata is associated with multilevel secure (MLS) systems. MLS systems mediate access by a subject to an object based on relative sensitivity levels. It follows that all subjects and objects in the scope of control of the MLS system are either directly labeled or indirectly attributed with sensitivity levels. The corollary of labeled metadata for MLS systems states that objects containing metadata are labeled. As with protection needs assessments for data, attention is given to ensure that the confidentiality and integrity protections are individually assessed, specified, and allocated to metadata, as would be done for mission, business, and system data.

Security and Privacy Engineering Principles | Self-analysis (SA-8(21))

Description for Security and Privacy Engineering Principles | Self-analysis (SA-8(21))
Implement the security design principle of self-analysis in [Assignment: organization-defined systems or system components].

Discussion for Security and Privacy Engineering Principles | Self-analysis (SA-8(21))
The principle of self-analysis states that a system component is able to assess its internal state and functionality to a limited extent at various stages of execution, and that this self-analysis capability is commensurate with the level of trustworthiness invested in the system. At the system level, 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 (to a limited extent) of higher-level components. For example, trusted boot sequences involve a trusted lower-level component that attests to the trustworthiness of the next higher-level components so that a transitive chain of trust can be established. At the root, a component attests to itself, which usually involves an axiomatic or environmentally enforced assumption about its integrity. Results of the self-analyses can be used to guard against externally induced errors, internal malfunction, or transient errors. By following this principle, some simple malfunctions or errors can be detected without allowing the effects of the error or malfunction to propagate outside of the component. Further, the self-test can be used to attest to the configuration of the component, detecting any potential conflicts in configuration with respect to the expected configuration.

Security and Privacy Engineering Principles | Accountability and Traceability (SA-8(22))

Description for Security and Privacy Engineering Principles | Accountability and Traceability (SA-8(22))
Implement the security design principle of accountability and traceability in [Assignment: organization-defined systems or system components].

Discussion for Security and Privacy Engineering Principles | Accountability and Traceability (SA-8(22))
The principle of accountability and traceability states that it is possible to trace security-relevant actions (i.e., subject-object interactions) to the entity on whose behalf 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., an audit subsystem). To record the details about actions, the system is able to uniquely identify the entity on whose behalf the action is being carried out and also record the relevant sequence of actions that are carried out. The accountability policy also requires that audit trail itself be protected from unauthorized access and modification. The principle of least privilege assists in tracing the actions to particular entities, as it increases the granularity of accountability. Associating specific actions with system entities, and ultimately with users, and making the audit trail secure against unauthorized access and modifications provide non-repudiation because once an action is recorded, it is not possible to change the audit trail. Another important function that accountability and traceability serves 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 the security policy.

Security and Privacy Engineering Principles | Secure Defaults (SA-8(23))

Description for Security and Privacy Engineering Principles | Secure Defaults (SA-8(23))
Implement the security design principle of secure defaults in [Assignment: organization-defined systems or system components].

Discussion for Security and Privacy Engineering Principles | Secure Defaults (SA-8(23))
The principle of secure defaults states that the default configuration of a system (including its constituent subsystems, components, and mechanisms) reflects a restrictive and conservative enforcement of security policy. The principle of secure defaults 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 that follow a deny unless explicitly authorized strategy. The initial configuration aspect of this principle requires that any as shipped configuration of a system, subsystem, or system component does not aid in the violation of the security policy and can prevent the system from operating in the default configuration for those cases where the security policy itself requires configuration by the operational user.
Restrictive defaults mean that the system will operate as-shipped with adequate self-protection and be able to prevent security breaches before the intended security policy and system configuration is established. In cases where the protection provided by the as-shipped product is inadequate, stakeholders assess the risk of using it prior to establishing a secure initial state. Adherence to the principle of secure defaults guarantees that a system is established in a secure state upon successfully completing initialization. In situations where the system fails to complete initialization, either it will perform a requested operation using secure defaults or it will not perform the operation. Refer to the principles of continuous protection and secure failure and recovery 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 insecure alternative is to allow a request unless it is shown to be inconsistent with the policy. In a large system, the conditions that are satisfied to grant a request that is denied by default are often far more compact and complete than those that would need to be checked in order to deny a request that is granted by default.

Security and Privacy Engineering Principles | Secure Failure and Recovery (SA-8(24))

Description for Security and Privacy Engineering Principles | Secure Failure and Recovery (SA-8(24))
Implement the security design principle of secure failure and recovery in [Assignment: organization-defined systems or system components].

Discussion for Security and Privacy Engineering Principles | Secure Failure and Recovery (SA-8(24))
The principle of secure failure and recovery states that neither a failure in a system function or mechanism nor any recovery action in response to failure leads to a violation of security policy. The principle of secure failure and recovery parallels the principle of continuous protection to ensure that a system is capable of detecting (within limits) actual and impending failure at any stage of its operation (i.e., initialization, normal operation, shutdown, and maintenance) and to take appropriate steps to ensure that security policies are not violated. In addition, when specified, the system is capable of recovering from impending or actual failure to resume normal, degraded, or alternative secure operations while ensuring that a secure state is maintained such that security policies are not violated.
Failure is a condition in which the behavior of a component deviates from its specified or expected behavior for an explicitly documented input. Once a failed security function is detected, the system may reconfigure itself to circumvent the failed component while maintaining security and provide all or part of the functionality of the original system, or it may completely shut itself down to prevent any further violation of security policies. For this to occur, the reconfiguration functions of the system are designed to ensure continuous enforcement of security policy during the various phases of reconfiguration.
Another technique that can be used to recover from failures is to perform a rollback to a secure state (which may be the initial state) and then either shutdown or replace the service or component that failed such that secure operations may resume. Failure of a component may or may not be detectable to the components using it. The principle of secure failure indicates that components fail in a state that denies rather than grants access. For example, a nominally atomic operation interrupted before completion does not violate security policy and is designed to handle interruption events by employing higher-level atomicity and rollback mechanisms (e.g., transactions). If a service is being used, its atomicity properties are well-documented and characterized so that the component availing itself of that service can detect and handle interruption events appropriately. For example, a system is designed to gracefully respond to disconnection and support resynchronization and data consistency after disconnection.
Failure protection strategies that employ replication of policy enforcement mechanisms, sometimes called defense in depth, can allow the system to continue

in a secure state even when one mechanism has failed to protect the system. If the mechanisms are similar, however, the additional protection may be illusory, as the adversary can simply attack in series. Similarly, in a networked system, breaking the security on one system or service may enable an attacker to do the same on other similar replicated systems and services. By employing multiple protection mechanisms whose features are significantly different, the possibility of attack replication or repetition can be reduced. Analyses are conducted to weigh the costs and benefits of such redundancy techniques against increased resource usage and adverse effects on the overall system performance. Additional analyses are conducted as the complexity of these mechanisms increases, as could be the case for dynamic behaviors. Increased complexity generally reduces trustworthiness. When a resource cannot be continuously protected, it is critical to detect and repair any security breaches before the resource is once again used in a secure context.

Security and Privacy Engineering Principles | Economic Security (SA-8(25))

Description for Security and Privacy Engineering Principles | Economic Security (SA-8(25))
Implement the security design principle of economic security in [Assignment: organization-defined systems or system components].

Discussion for Security and Privacy Engineering Principles | Economic Security (SA-8(25))
The principle of economic security states that security mechanisms are not costlier than the potential damage that could occur from a security breach. This is the security-relevant form of the cost-benefit analyses used in risk management. The cost assumptions of cost-benefit analysis prevent the system designer from incorporating security mechanisms of greater strength than necessary, where strength of mechanism is proportional to cost. The principle of economic security also requires analysis of the benefits of assurance relative to the cost of that assurance in terms of the effort expended to obtain relevant and credible evidence as well as the necessary analyses to assess and draw trustworthiness and risk conclusions from the evidence.

Security and Privacy Engineering Principles | Performance Security (SA-8(26))

Description for Security and Privacy Engineering Principles | Performance Security (SA-8(26))
Implement the security design principle of performance security in [Assignment: organization-defined systems or system components].

Discussion for Security and Privacy Engineering Principles | Performance Security (SA-8(26))
The principle of performance security states that security mechanisms are constructed so that they do not degrade system performance unnecessarily. Stakeholder and system design requirements for performance and security are precisely articulated and prioritized. For the system implementation to meet its design requirements and be found acceptable to stakeholders (i.e., validation against stakeholder requirements), the designers adhere to the specified constraints that capability performance needs place on protection needs. The overall impact of computationally intensive security services (e.g., cryptography) are assessed and demonstrated to pose no significant impact to higher-priority performance considerations or are deemed to provide an acceptable trade-off of performance for trustworthy protection. The trade-off considerations include less computationally intensive security services unless they are unavailable or insufficient. The insufficiency of a security service is determined by functional capability and strength of mechanism. The strength of mechanism is selected with respect to security requirements, performance-critical overhead issues (e.g., cryptographic key management), and an assessment of the capability of the threat. The principle of performance security leads to the incorporation of features that help in the enforcement of security policy but incur minimum overhead, such as low-level hardware mechanisms upon which higher-level services can be built. Such low-level mechanisms are usually very specific, have very limited functionality, and are optimized for performance. For example, once access rights to a portion of memory is granted, many systems use hardware mechanisms to ensure that all further accesses involve the correct memory address and access mode. Application of this principle reinforces the need to design security into the system from the ground up and to incorporate simple mechanisms at the lower layers that can be used as building blocks for higher-level mechanisms.

Security and Privacy Engineering Principles | Human Factored Security (SA-8(27))

Description for Security and Privacy Engineering Principles | Human Factored Security (SA-8(27))
Implement the security design principle of human factored security in [Assignment: organization-defined systems or system components].

Discussion for Security and Privacy Engineering Principles | Human Factored Security (SA-8(27))
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 that affect such policy and its 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 provide the user with meaningful, clear, and relevant feedback and warnings when insecure choices are being made. Particular attention is given to interfaces through which personnel responsible for system administration and operation configure and set up the security policies. Ideally, these personnel are able to understand the impact of their choices. Personnel with system administrative and operational responsibilities are able to configure systems before start-up and administer them during runtime with confidence that their intent is correctly mapped to the system's mechanisms. Security services, functions, and mechanisms do not impede or unnecessarily complicate the intended use of the system. There is a trade-off between system usability and the strictness necessary for security policy enforcement. If security mechanisms are frustrating or difficult to use, then users may disable them, avoid them, or use them in ways inconsistent with the security requirements and protection needs that the mechanisms were designed to satisfy.

Security and Privacy Engineering Principles | Acceptable Security (SA-8(28))

Description for Security and Privacy Engineering Principles | Acceptable Security (SA-8(28))
Implement the security design principle of acceptable security in [Assignment: organization-defined systems or system components].

Discussion for Security and Privacy Engineering Principles | Acceptable Security (SA-8(28))
The principle of acceptable security requires that the level of privacy and performance that the system provides is consistent with the users' expectations. The perception of personal privacy may affect user behavior, morale, and effectiveness. Based on the organizational privacy policy and the system design, users should be able to restrict their actions to protect their privacy. When systems fail to provide intuitive interfaces or meet privacy and performance expectations, users may either choose to completely avoid the system or use it in ways that may be inefficient or even insecure.

Security and Privacy Engineering Principles | Repeatable and Documented Procedures (SA-8(29))

Description for Security and Privacy Engineering Principles | Repeatable and Documented Procedures (SA-8(29))
Implement the security design principle of repeatable and documented procedures in [Assignment: organization-defined systems or system components].

Discussion for Security and Privacy Engineering Principles | Repeatable and Documented Procedures (SA-8(29))
The principle of repeatable and documented procedures states that the techniques and methods employed to construct a system component permit the same component to be completely and correctly reconstructed at a later time. Repeatable and documented procedures support the development of a component that is identical to the component created earlier, which may be in widespread use. In the case of other system artifacts (e.g., documentation and testing results), repeatability supports consistency and the ability to inspect the artifacts. Repeatable and documented procedures can be introduced at various stages within the system development life cycle and contribute to the ability to evaluate assurance claims for the system. Examples include systematic procedures for code development and review, procedures for the configuration management of development tools and system artifacts, and procedures for system delivery.

Security and Privacy Engineering Principles | Procedural Rigor (SA-8(30))

Description for Security and Privacy Engineering Principles | Procedural Rigor (SA-8(30))
Implement the security design principle of procedural rigor in [Assignment: organization-defined systems or system components].

Discussion for Security and Privacy Engineering Principles | Procedural Rigor (SA-8(30))
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 unspecified 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 as it has been built rather than trusting that the component, as implemented, is the authoritative (and potentially misleading) specification.
Finally, modifications to an existing system component are easier when there are detailed specifications that describe its current design instead of studying source code or schematics to try to understand how it works. Procedural rigor helps ensure that security functional 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 commensurate 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 merited.

Security and Privacy Engineering Principles | Secure System Modification (SA-8(31))

Description for Security and Privacy Engineering Principles | Secure System Modification (SA-8(31))
Implement the security design principle of secure system modification in [Assignment: organization-defined systems or system components].

Discussion for Security and Privacy Engineering Principles | Secure System Modification (SA-8(31))
The principle of secure system modification states that system modification maintains system security with respect to the security requirements and risk tolerance of stakeholders. Upgrades or modifications to systems can transform secure systems into systems that are not secure. The procedures for system modification ensure that if the system is to maintain its trustworthiness, the same rigor that was applied to its initial development is applied to any system changes. 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 parallels the principle of secure evolvability.

Security and Privacy Engineering Principles | Sufficient Documentation (SA-8(32))

Description for Security and Privacy Engineering Principles | Sufficient Documentation (SA-8(32))
Implement the security design principle of sufficient documentation in [Assignment: organization-defined systems or system components].

Discussion for Security and Privacy Engineering Principles | Sufficient Documentation (SA-8(32))
The principle of sufficient documentation states that organizational personnel with responsibilities to interact with the system are provided with adequate documentation and other information such that the personnel contribute to rather than detract from system security. Despite attempts to comply with principles such as human factored security and acceptable security, systems are inherently complex, and the design intent for the use of security mechanisms and the ramifications of the misuse or misconfiguration of security mechanisms are not always intuitively obvious. Uninformed and insufficiently trained users can introduce vulnerabilities due to errors of omission and commission. The availability of documentation and training can help to ensure a knowledgeable cadre of personnel, all of whom have a critical role in the achievement of principles such as continuous protection. Documentation is written clearly and supported by training that provides security awareness and understanding of security-relevant responsibilities.

Security and Privacy Engineering Principles | Minimization (SA-8(33))

Description for Security and Privacy Engineering Principles | Minimization (SA-8(33))
Implement the privacy principle of minimization using [Assignment: organization-defined processes].

Discussion for Security and Privacy Engineering Principles | Minimization (SA-8(33))
The principle of minimization states that organizations should only process personally identifiable information that is directly relevant and necessary to accomplish an authorized purpose and should only maintain personally identifiable information for as long as is necessary to accomplish the purpose. Organizations have processes in place, consistent with applicable laws and policies, to implement the principle of minimization.

External System Services (SA-9)

Description for External System Services (SA-9)
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].

Discussion for External System Services (SA-9)
External system services are provided by an external provider, and the organization has no direct control over the implementation of the 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, interagency agreements, lines of business arrangements, licensing agreements, joint ventures, and supply chain exchanges. The responsibility for managing risks from the use of external system services remains with authorizing officials. For services external to organizations, a chain of trust requires that organizations establish and retain a certain level of confidence that each provider in the consumer-provider relationship provides adequate protection for the services rendered. The extent and nature of this chain of trust vary based on relationships between organizations and the external providers. Organizations document the basis for the trust relationships so that the relationships can be monitored. External system services documentation includes government, service providers, end user security roles and responsibilities, and service-level agreements. Service-level agreements define the expectations of performance for implemented controls, describe measurable outcomes, and identify remedies and response requirements for identified instances of noncompliance.

External System Services | Risk Assessments and Organizational Approvals (SA-9(1))

Description for External System Services | Risk Assessments and Organizational Approvals (SA-9(1))
(a) Conduct an organizational assessment of risk prior to the acquisition or outsourcing of information security services; and
(b) Verify that the acquisition or outsourcing of dedicated information security services is approved by [Assignment: organization-defined personnel or roles].

Discussion for External System Services | Risk Assessments and Organizational Approvals (SA-9(1))
Information security services include the operation of security devices, such as firewalls or key management services as well as incident monitoring, analysis, and response. Risks assessed can include system, mission or business, security, privacy, or supply chain risks.

External System Services | Identification of Functions, Ports, Protocols, and Services (SA-9(2))

Description for External System Services | Identification of Functions, Ports, Protocols, and Services (SA-9(2))
Require providers of the following external system services to identify the functions, ports, protocols, and other services required for the use of such services: [Assignment: organization-defined external system services].

Discussion for External System Services | Identification of Functions, Ports, Protocols, and Services (SA-9(2))
Information from external service providers regarding the specific functions, ports, protocols, and services used in the provision of such services can be useful when the need arises to understand the trade-offs involved in restricting certain functions and services or blocking certain ports and protocols.

External System Services | Establish and Maintain Trust Relationship with Providers (SA-9(3))

Description for External System Services | Establish and Maintain Trust Relationship with Providers (SA-9(3))
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].

Discussion for External System Services | Establish and Maintain Trust Relationship with Providers (SA-9(3))
Trust relationships between organizations and external service providers reflect the degree of confidence that the risk from using external services is at an acceptable level. Trust relationships can help organizations gain increased levels of confidence that service providers are providing adequate protection for the services rendered and can also be useful when conducting incident response or when planning for upgrades or obsolescence. Trust relationships can be complicated due to the potentially large number of entities participating in the consumer-provider interactions, subordinate relationships 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 that 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.

External System Services | Consistent Interests of Consumers and Providers (SA-9(4))

Description for External System Services | Consistent Interests of Consumers and Providers (SA-9(4))
Take the following actions to verify that the interests of [Assignment: organization-defined external service providers] are consistent with and reflect organizational interests: [Assignment: organization-defined actions].

Discussion for External System Services | Consistent Interests of Consumers and Providers (SA-9(4))
As organizations increasingly use external service providers, it is possible that the interests of the service providers may diverge from organizational interests. In such situations, simply having the required technical, management, or operational controls in place may not be sufficient if the providers that implement and manage those controls are not operating in a manner consistent with the interests of the consuming organizations. Actions that organizations take to address such concerns include requiring background checks for selected service provider personnel; examining ownership records; employing only trustworthy service providers, such as providers with which organizations have had successful trust relationships; and conducting routine, periodic, unscheduled visits to service provider facilities.

External System Services | Processing, Storage, and Service Location (SA-9(5))

Description for External System Services | Processing, Storage, and Service Location (SA-9(5))
Restrict the location of [Selection (one or more): information processing; information or data; system services] to [Assignment: organization-defined locations] based on [Assignment: organization-defined requirements or conditions].

Discussion for External System Services | Processing, Storage, and Service Location (SA-9(5))
The location of information processing, information and data storage, or system services can have a direct impact on the ability of organizations to successfully execute their mission and business functions. The impact occurs when external providers control the location of processing, storage, or services. The criteria that external providers use for the selection of processing, storage, or service locations may be different from the criteria that organizations use. For example, organizations may desire that data or information storage locations be restricted to certain locations to help facilitate incident response activities in case of information security incidents or breaches. Incident response activities, including forensic analyses and after-the-fact investigations, may be adversely affected by the governing laws, policies, or protocols in the locations where processing and storage occur and/or the locations from which system services emanate.

External System Services | Organization-controlled Cryptographic Keys (SA-9(6))

Description for External System Services | Organization-controlled Cryptographic Keys (SA-9(6))
Maintain exclusive control of cryptographic keys for encrypted material stored or transmitted through an external system.

Discussion for External System Services | Organization-controlled Cryptographic Keys (SA-9(6))
Maintaining exclusive control of cryptographic keys in an external system prevents decryption of organizational data by external system staff. Organizational control of cryptographic keys can be implemented by encrypting and decrypting data inside the organization as data is sent to and received from the external system or by employing a component that permits encryption and decryption functions to be local to the external system but allows exclusive organizational access to the encryption keys.

External System Services | Organization-controlled Integrity Checking (SA-9(7))

Description for External System Services | Organization-controlled Integrity Checking (SA-9(7))
Provide the capability to check the integrity of information while it resides in the external system.

Discussion for External System Services | Organization-controlled Integrity Checking (SA-9(7))
Storage of organizational information in an external system could limit visibility into the security status of its data. The ability of the organization to verify and validate the integrity of its stored data without transferring it out of the external system provides such visibility.

External System Services | Processing and Storage Location — U.S. Jurisdiction (SA-9(8))

Description for External System Services | Processing and Storage Location — U.S. Jurisdiction (SA-9(8))
Restrict the geographic location of information processing and data storage to facilities located within in the legal jurisdictional boundary of the United States.

Discussion for External System Services | Processing and Storage Location — U.S. Jurisdiction (SA-9(8))
The geographic location of information processing and data storage can have a direct impact on the ability of organizations to successfully execute their mission and business functions. A compromise or breach of high impact information and systems can have severe or catastrophic adverse impacts 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.

Developer Configuration Management (SA-10)

Description for Developer Configuration Management (SA-10)
Require the developer of the system, system component, or system service to:
a. Perform configuration management during system, component, or service [Selection (one 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. Document 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].

Discussion for Developer Configuration Management (SA-10)
Organizations consider the quality and completeness of configuration management activities conducted by developers as direct evidence of applying effective security controls. Controls include protecting the master copies of material used to generate security-relevant portions of the system hardware, software, and firmware from unauthorized modification or destruction. Maintaining the integrity of changes to the system, system component, or system service requires strict configuration control throughout the system development life cycle to track authorized changes and prevent unauthorized changes.
The configuration items that are placed under configuration management include the 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.

Developer Configuration Management | Software and Firmware Integrity Verification (SA-10(1))

Description for Developer Configuration Management | Software and Firmware Integrity Verification (SA-10(1))
Require the developer of the system, system component, or system service to enable integrity verification of software and firmware components.

Discussion for Developer Configuration Management | Software and Firmware Integrity Verification (SA-10(1))
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 mechanisms 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.

Developer Configuration Management | Alternative Configuration Management Processes (SA-10(2))

Description for Developer Configuration Management | Alternative Configuration Management Processes (SA-10(2))
Provide an alternate configuration management process using organizational personnel in the absence of a dedicated developer configuration management team.

Discussion for Developer Configuration Management | Alternative Configuration Management Processes (SA-10(2))
Alternate configuration management processes may be required when organizations use commercial off-the-shelf information technology products. Alternate configuration management processes include organizational personnel who review and approve proposed changes to systems, system components, and system services and conduct security and privacy impact analyses prior to the implementation of changes to systems, components, or services.

Developer Configuration Management | Hardware Integrity Verification (SA-10(3))

Description for Developer Configuration Management | Hardware Integrity Verification (SA-10(3))
Require the developer of the system, system component, or system service to enable integrity verification of hardware components.

Discussion for Developer Configuration Management | Hardware Integrity Verification (SA-10(3))
Hardware integrity verification allows organizations to detect unauthorized changes to hardware components using developer-provided tools, techniques, methods, and mechanisms. Organizations may verify the integrity of hardware components with hard-to-copy labels, verifiable serial numbers provided by developers, and by requiring the use of anti-tamper technologies. Delivered hardware components also include hardware and firmware updates to such components.

Developer Configuration Management | Trusted Generation (SA-10(4))

Description for Developer Configuration Management | Trusted Generation (SA-10(4))
Require the developer of the system, 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.

Discussion for Developer Configuration Management | Trusted Generation (SA-10(4))
The trusted generation of descriptions, source code, and object code addresses authorized 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(3) allow organizations to detect unauthorized changes to hardware, software, and firmware components using tools, techniques, or mechanisms provided by developers.

Developer Configuration Management | Mapping Integrity for Version Control (SA-10(5))

Description for Developer Configuration Management | Mapping Integrity for Version Control (SA-10(5))
Require the developer of the system, system component, or system service to maintain the integrity of the mapping between the master build data describing the current version of security-relevant hardware, software, and firmware and the on-site master copy of the data for the current version.

Discussion for Developer Configuration Management | Mapping Integrity for Version Control (SA-10(5))
Mapping integrity for version control addresses changes to hardware, software, and firmware components during both initial development and system development life cycle updates. Maintaining the integrity between the master copies of security-relevant hardware, software, and firmware (including designs, hardware drawings, source code) and the equivalent data in master copies in operational environments is essential to ensuring the availability of organizational systems that support critical mission and business functions.

Developer Configuration Management | Trusted Distribution (SA-10(6))

Description for Developer Configuration Management | Trusted Distribution (SA-10(6))
Require the developer of the system, system component, or system service to execute procedures for ensuring that security-relevant hardware, software, and firmware updates distributed to the organization are exactly as specified by the master copies.

Discussion for Developer Configuration Management | Trusted Distribution (SA-10(6))
The trusted distribution of security-relevant hardware, software, and firmware updates help to ensure that the updates are correct representations of the master copies maintained by the developer and have not been tampered with during distribution.

Developer Configuration Management | Security and Privacy Representatives (SA-10(7))

Description for Developer Configuration Management | Security and Privacy Representatives (SA-10(7))
Require [Assignment: organization-defined security and privacy representatives] to be included in the [Assignment: organization-defined configuration change management and control process].

Discussion for Developer Configuration Management | Security and Privacy Representatives (SA-10(7))
Information security and privacy representatives can include system security officers, senior agency information security officers, senior agency officials for privacy, and system privacy officers. Representation by personnel with information security and privacy expertise is important because changes to system configurations can have unintended side effects, some of which may be security- or privacy-relevant. Detecting such changes early in the process can help avoid unintended, negative consequences that could ultimately affect the security and privacy posture of systems. The configuration change management and control process in this control enhancement refers to the change management and control process defined by organizations in SA-10b.

Developer Testing and Evaluation (SA-11)

Description for Developer Testing and Evaluation (SA-11)
Require the developer of the system, system component, or system service, at all post-design stages of the system development life cycle, to:
a. Develop and implement a plan for ongoing security and privacy control assessments;
b. Perform [Selection (one or more): unit; integration; system; regression] testing/evaluation [Assignment: organization-defined frequency] at [Assignment: organization-defined depth and coverage];
c. Produce evidence of the execution of the assessment plan and the results of the testing and evaluation;
d. Implement a verifiable flaw remediation process; and
e. Correct flaws identified during testing and evaluation.

Discussion for Developer Testing and Evaluation (SA-11)
Developmental testing and evaluation confirms that the required controls are implemented correctly, operating as intended, enforcing the desired security and privacy policies, and meeting established security and privacy requirements. Security properties of systems and the privacy of individuals may be affected by the interconnection of system components or changes to those components. The interconnections or changes—including upgrading or replacing applications, operating systems, and firmware—may adversely affect previously implemented controls. Ongoing assessment during development allows for additional types of testing and evaluation that developers can conduct to reduce or eliminate potential flaws. Testing custom software applications may require approaches such as manual code review, security architecture review, and penetration testing, as well as and static analysis, dynamic analysis, binary analysis, or a hybrid of the three analysis approaches.
Developers can use the analysis approaches, along with security instrumentation and fuzzing, in a variety of tools and in source code reviews. The security and privacy assessment plans include the specific activities that developers plan to carry out, including the types of analyses, testing, evaluation, and reviews of software and firmware components; the degree of rigor to be applied; the frequency of the ongoing testing and evaluation; and the types of artifacts produced during those processes. The depth of testing and evaluation refers to the rigor and level of detail associated with the assessment process. The coverage of testing and evaluation refers to the scope (i.e., number and type) of the artifacts included in the assessment process. Contracts specify the acceptance criteria for security and privacy assessment plans, flaw remediation processes, and the evidence that the plans and processes have been diligently applied. Methods for reviewing and protecting assessment plans, evidence, and documentation are commensurate with the security category or classification level of the system. Contracts may specify protection requirements for documentation.

Developer Testing and Evaluation | Static Code Analysis (SA-11(1))

Description for Developer Testing and Evaluation | Static Code Analysis (SA-11(1))
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.

Discussion for Developer Testing and Evaluation | Static Code Analysis (SA-11(1))
Static code analysis provides a technology and methodology for security reviews and includes checking for weaknesses in the code as well as for the incorporation of libraries or other included code with known vulnerabilities or that are out-of-date and not supported. Static code analysis can be used to identify vulnerabilities and enforce secure coding practices. It is most effective when used early in the development process, when each code change can automatically be scanned for potential weaknesses. Static code analysis can provide clear remediation guidance and identify defects for developers to fix. Evidence of the correct implementation of static analysis can include aggregate defect density for critical defect types, evidence that defects were inspected by developers or security professionals, and evidence that defects were remediated. A high density of ignored findings, 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.

Developer Testing and Evaluation | Threat Modeling and Vulnerability Analyses (SA-11(2))

Description for Developer Testing and Evaluation | Threat Modeling and Vulnerability Analyses (SA-11(2))
Require the developer of the system, system component, or system service to perform threat modeling and vulnerability analyses 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, known or assumed threats, and acceptable risk levels];
(b) Employs 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].

Discussion for Developer Testing and Evaluation | Threat Modeling and Vulnerability Analyses (SA-11(2))
Systems, system components, and system services may deviate significantly from the functional and design specifications created during the requirements and design stages of the system development life cycle. Therefore, updates to threat modeling and vulnerability analyses of those systems, system components, and system services during development and prior to delivery are critical to the effective operation of those systems, components, and services. Threat modeling and vulnerability analyses at this stage of the system development life cycle ensure that design and implementation changes have been accounted for and that vulnerabilities created because of those changes have been reviewed and mitigated.

Developer Testing and Evaluation | Independent Verification of Assessment Plans and Evidence (SA-11(3))

Description for Developer Testing and Evaluation | Independent Verification of Assessment Plans and Evidence (SA-11(3))
(a) Require an independent agent satisfying [Assignment: organization-defined independence criteria] to verify the correct implementation of the developer security and privacy assessment plans and the evidence produced during testing and evaluation; and
(b) Verify that the independent agent is provided with sufficient information to complete the verification process or granted the authority to obtain such information.

Discussion for Developer Testing and Evaluation | Independent Verification of Assessment Plans and Evidence (SA-11(3))
Independent agents have the qualifications—including the expertise, skills, training, certifications, and experience—to verify the correct implementation of developer security and privacy assessment plans.

Developer Testing and Evaluation | Manual Code Reviews (SA-11(4))

Description for Developer Testing and Evaluation | Manual Code Reviews (SA-11(4))
Require the developer of the system, system component, or system service to perform a manual code review of [Assignment: organization-defined specific code] using the following processes, procedures, and/or techniques: [Assignment: organization-defined processes, procedures, and/or techniques].

Discussion for Developer Testing and Evaluation | Manual Code Reviews (SA-11(4))
Manual code reviews are usually reserved for the critical software and firmware components of systems. Manual code reviews are effective at identifying weaknesses that require knowledge of the application's requirements or context that, in most cases, is unavailable to automated analytic tools and techniques, such as static and dynamic analysis. The benefits of manual code review include the ability to verify access control matrices against application controls and review detailed aspects of cryptographic implementations and controls.

Developer Testing and Evaluation | Penetration Testing (SA-11(5))

Description for Developer Testing and Evaluation | Penetration Testing (SA-11(5))
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) Under the following constraints: [Assignment: organization-defined constraints].

Discussion for Developer Testing and Evaluation | Penetration Testing (SA-11(5))
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 the implemented security and privacy features of information technology products and systems. Useful information for assessors who conduct penetration testing includes product and system design specifications, source code, and administrator and operator manuals. Penetration testing can include white-box, gray-box, or black-box testing with analyses performed by skilled professionals who simulate adversary actions. The objective of penetration testing is to discover vulnerabilities in systems, system components, and services that result from implementation errors, configuration faults, or other operational weaknesses or deficiencies. Penetration tests can be performed in conjunction with automated and manual code reviews to provide a greater level of analysis than would ordinarily be possible. When user session information and other personally identifiable information is captured or recorded during penetration testing, such information is handled appropriately to protect privacy.

Developer Testing and Evaluation | Attack Surface Reviews (SA-11(6))

Description for Developer Testing and Evaluation | Attack Surface Reviews (SA-11(6))
Require the developer of the system, system component, or system service to perform attack surface reviews.

Discussion for Developer Testing and Evaluation | Attack Surface Reviews (SA-11(6))
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 deficiencies 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 vectors generated as a result of the changes. The correction of identified flaws includes deprecation of unsafe functions.

Developer Testing and Evaluation | Verify Scope of Testing and Evaluation (SA-11(7))

Description for Developer Testing and Evaluation | Verify Scope of Testing and Evaluation (SA-11(7))
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].

Discussion for Developer Testing and Evaluation | Verify Scope of Testing and Evaluation (SA-11(7))
Verifying that testing and evaluation provides complete coverage of required controls can be accomplished by a variety of analytic techniques ranging from informal to formal. Each of these techniques provides an increasing level of assurance that corresponds to the degree of formality of the analysis. Rigorously demonstrating control coverage at the highest levels of assurance can be achieved using formal modeling and analysis techniques, including correlation between control implementation and corresponding test cases.

Developer Testing and Evaluation | Dynamic Code Analysis (SA-11(8))

Description for Developer Testing and Evaluation | Dynamic Code Analysis (SA-11(8))
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.

Discussion for Developer Testing and Evaluation | Dynamic Code Analysis (SA-11(8))
Dynamic code analysis provides runtime 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 runtime tools to ensure that security functionality performs in the way it was designed. A type of dynamic analysis, known as fuzz testing, induces program failures by deliberately introducing malformed or random data into software programs. Fuzz testing strategies are derived from the intended use of applications and the functional and design specifications for the applications. To understand the scope of dynamic code analysis and the assurance provided, organizations may also consider conducting code coverage analysis (i.e., checking the degree to which the code has been tested using metrics such as percent of subroutines tested or percent of program statements called during execution of the test suite) and/or

concordance analysis (i.e., checking for words that are out of place in software code, such as non-English language words or derogatory terms).

Developer Testing and Evaluation | Interactive Application Security Testing (SA-11(9))

Description for Developer Testing and Evaluation | Interactive Application Security Testing (SA-11(9))
Require the developer of the system, system component, or system service to employ interactive application security testing tools to identify flaws and document the results.

Discussion for Developer Testing and Evaluation | Interactive Application Security Testing (SA-11(9))
Interactive (also known as instrumentation-based) application security testing is a method of detecting vulnerabilities by observing applications as they run during testing. The use of instrumentation relies on direct measurements of the actual running applications and uses access to the code, user interaction, libraries, frameworks, backend connections, and configurations to directly measure control effectiveness. When combined with analysis techniques, interactive application security testing can identify a broad range of potential vulnerabilities and confirm control effectiveness. Instrumentation-based testing works in real time and can be used continuously throughout the system development life cycle.

Supply Chain Protection | Supplier Reviews (SA-12(2))

Description for Supply Chain Protection | Supplier Reviews (SA-12(2))
[Withdrawn: Moved to SR-6.]

Discussion for Supply Chain Protection | Supplier Reviews (SA-12(2))

Supply Chain Protection | Trusted Shipping and Warehousing (SA-12(3))

Description for Supply Chain Protection | Trusted Shipping and Warehousing (SA-12(3))
[Withdrawn: Incorporated into SR-3.]

Discussion for Supply Chain Protection | Trusted Shipping and Warehousing (SA-12(3))

Supply Chain Protection | Diversity of Suppliers (SA-12(4))

Description for Supply Chain Protection | Diversity of Suppliers (SA-12(4))
[Withdrawn: Moved to SR-3(1).]

Discussion for Supply Chain Protection | Diversity of Suppliers (SA-12(4))

Supply Chain Protection | Limitation of Harm (SA-12(5))

Description for Supply Chain Protection | Limitation of Harm (SA-12(5))
[Withdrawn: Moved to SR-3(2).]

Discussion for Supply Chain Protection | Limitation of Harm (SA-12(5))

Supply Chain Protection | Minimizing Procurement Time (SA-12(6))

Description for Supply Chain Protection | Minimizing Procurement Time (SA-12(6))
[Withdrawn: Incorporated into SR-5(1).]

Discussion for Supply Chain Protection | Minimizing Procurement Time (SA-12(6))

Supply Chain Protection | Assessments Prior to Selection / Acceptance / Update (SA-12(7))

Description for Supply Chain Protection | Assessments Prior to Selection / Acceptance / Update (SA-12(7))
[Withdrawn: Moved to SR-5(2).]

Discussion for Supply Chain Protection | Assessments Prior to Selection / Acceptance / Update (SA-12(7))

Supply Chain Protection | Use of All-source Intelligence (SA-12(8))

Description for Supply Chain Protection | Use of All-source Intelligence (SA-12(8))
[Withdrawn: Incorporated into RA-3(2).]

Discussion for Supply Chain Protection | Use of All-source Intelligence (SA-12(8))

Supply Chain Protection | Operations Security (SA-12(9))

Description for Supply Chain Protection | Operations Security (SA-12(9))
[Withdrawn: Moved to SR-7.]

Discussion for Supply Chain Protection | Operations Security (SA-12(9))

Trustworthiness (SA-13)

Description for Trustworthiness (SA-13)
[Withdrawn: Incorporated into SA-8.]

Discussion for Trustworthiness (SA-13)

Criticality Analysis (SA-14)

Description for Criticality Analysis (SA-14)
[Withdrawn: Incorporated into RA-9.]

Discussion for Criticality Analysis (SA-14)

Criticality Analysis | Critical Components with No Viable Alternative Sourcing (SA-14(1))

Description for Criticality Analysis | Critical Components with No Viable Alternative Sourcing (SA-14(1))
[Withdrawn: Incorporated into SA-20.]

Discussion for Criticality Analysis | Critical Components with No Viable Alternative Sourcing (SA-14(1))

Development Process, Standards, and Tools | Threat Modeling and Vulnerability Analysis (SA-15(4))

Description for Development Process, Standards, and Tools | Threat Modeling and Vulnerability Analysis (SA-15(4))
[Withdrawn: Incorporated into SA-11(2).]

Discussion for Development Process, Standards, and Tools | Threat Modeling and Vulnerability Analysis (SA-15(4))

Development Process, Standards, and Tools | Use of Live Data (SA-15(9))

Description for Development Process, Standards, and Tools | Use of Live Data (SA-15(9))
[Withdrawn: Incorporated into SA-3(2).]

Discussion for Development Process, Standards, and Tools | Use of Live Data (SA-15(9))

Tamper Resistance and Detection (SA-18)

Description for Tamper Resistance and Detection (SA-18)
[Withdrawn: Moved to SR-9.]

Discussion for Tamper Resistance and Detection (SA-18)

Tamper Resistance and Detection | Multiple Phases of System Development Life Cycle (SA-18(1))

Description for Tamper Resistance and Detection | Multiple Phases of System Development Life Cycle (SA-18(1))
[Withdrawn: Moved to SR-9(1).]

Discussion for Tamper Resistance and Detection | Multiple Phases of System Development Life Cycle (SA-18(1))

Tamper Resistance and Detection | Inspection of Systems or Components (SA-18(2))

Description for Tamper Resistance and Detection | Inspection of Systems or Components (SA-18(2))
[Withdrawn: Moved to SR-10.]

Discussion for Tamper Resistance and Detection | Inspection of Systems or Components (SA-18(2))

Component Authenticity (SA-19)

Description for Component Authenticity (SA-19)
[Withdrawn: Moved to SR-11.]

Discussion for Component Authenticity (SA-19)

Component Authenticity | Anti-counterfeit Training (SA-19(1))

Description for Component Authenticity | Anti-counterfeit Training (SA-19(1))
[Withdrawn: Moved to SR-11(1).]

Discussion for Component Authenticity | Anti-counterfeit Training (SA-19(1))

Component Authenticity | Configuration Control for Component Service and Repair (SA-19(2))

Description for Component Authenticity | Configuration Control for Component Service and Repair (SA-19(2))
[Withdrawn: Moved to SR-11(2).]

Discussion for Component Authenticity | Configuration Control for Component Service and Repair (SA-19(2))

Development Process, Standards, and Tools (SA-15)

Description for Development Process, Standards, and Tools (SA-15)
a. Require the developer of the system, system component, or system service to follow a documented development process that:
1. Explicitly addresses security and privacy requirements;
2. Identifies the standards and tools used in the development process;
3. Documents the specific tool options and tool configurations used in the development process; and
4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and
b. Review 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 for Development Process, Standards, and Tools (SA-15)
Development tools include programming languages and computer-aided design systems. Reviews 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 processes facilitates effective supply chain risk assessment and mitigation. Such integrity requires configuration control throughout the system development life cycle to track authorized changes and prevent unauthorized changes.

Development Process, Standards, and Tools | Quality Metrics (SA-15(1))

Description for Development Process, Standards, and Tools | Quality Metrics (SA-15(1))
Require the developer of the system, system component, or system service to:
(a) Define quality metrics at the beginning of the development process; and
(b) Provide evidence of meeting the quality metrics [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined program review milestones]; upon delivery].

Discussion for Development Process, Standards, and Tools | Quality Metrics (SA-15(1))
Organizations use quality metrics to establish acceptable levels of system quality. Metrics can include quality gates, which are collections of completion criteria or sufficiency standards that represent the satisfactory execution of specific phases of the system development project. For example, a quality gate may require the elimination of all compiler warnings or a determination that such warnings have no impact on the effectiveness of required security or privacy capabilities. During the execution phases of development projects, quality gates provide clear, unambiguous indications of progress. Other metrics apply to the entire

development project. Metrics can include defining the severity thresholds of vulnerabilities in accordance with organizational risk tolerance, such as requiring no known vulnerabilities in the delivered system with a Common Vulnerability Scoring System (CVSS) severity of medium or high.

Development Process, Standards, and Tools | Security and Privacy Tracking Tools (SA-15(2))

Description for Development Process, Standards, and Tools | Security and Privacy Tracking Tools (SA-15(2))
Require the developer of the system, system component, or system service to select and employ security and privacy tracking tools for use during the development process.

Discussion for Development Process, Standards, and Tools | Security and Privacy Tracking Tools (SA-15(2))
System development teams select and deploy security and privacy tracking tools, including vulnerability or work item tracking systems that facilitate assignment, sorting, filtering, and tracking of completed work items or tasks associated with development processes.

Development Process, Standards, and Tools | Criticality Analysis (SA-15(3))

Description for Development Process, Standards, and Tools | Criticality Analysis (SA-15(3))
Require the developer of the system, system component, or system service to perform a criticality analysis:
(a) At the following decision points in the system development life cycle: [Assignment: organization-defined decision points in the system development life cycle]; and
(b) At the following level of rigor: [Assignment: organization-defined breadth and depth of criticality analysis].

Discussion for Development Process, Standards, and Tools | Criticality Analysis (SA-15(3))
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, 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.

Component Authenticity | Component Disposal (SA-19(3))

Description for Component Authenticity | Component Disposal (SA-19(3))
[Withdrawn: Moved to SR-12.]

Discussion for Component Authenticity | Component Disposal (SA-19(3))

Development Process, Standards, and Tools | Attack Surface Reduction (SA-15(5))

Description for Development Process, Standards, and Tools | Attack Surface Reduction (SA-15(5))
Require the developer of the system, system component, or system service to reduce attack surfaces to [Assignment: organization-defined thresholds].

Discussion for Development Process, Standards, and Tools | Attack Surface Reduction (SA-15(5))
Attack surface reduction is closely aligned with threat and vulnerability analyses and system architecture and design. Attack surface reduction is a means of reducing risk to organizations by giving attackers less opportunity to exploit weaknesses or deficiencies (i.e., potential vulnerabilities) within systems, system components, and system services. Attack surface reduction includes implementing the concept of layered defenses, applying the principles of least privilege and least functionality, applying secure software development practices, deprecating unsafe functions, reducing entry points available to unauthorized users, reducing the amount of code that executes, and eliminating application programming interfaces (APIs) that are vulnerable to attacks.

Development Process, Standards, and Tools | Continuous Improvement (SA-15(6))

Description for Development Process, Standards, and Tools | Continuous Improvement (SA-15(6))
Require the developer of the system, system component, or system service to implement an explicit process to continuously improve the development process.

Discussion for Development Process, Standards, and Tools | Continuous Improvement (SA-15(6))
Developers of systems, system components, and system services consider the effectiveness and efficiency of their development processes for meeting quality objectives and addressing the security and privacy capabilities in current threat environments.

Development Process, Standards, and Tools | Automated Vulnerability Analysis (SA-15(7))

Description for Development Process, Standards, and Tools | Automated Vulnerability Analysis (SA-15(7))
Require the developer of the system, system component, or system service [Assignment: organization-defined frequency] to:
(a) Perform an automated vulnerability analysis using [Assignment: organization-defined tools];
(b) Determine the exploitation potential for discovered vulnerabilities;
(c) Determine potential risk mitigations for delivered vulnerabilities; and
(d) Deliver the outputs of the tools and results of the analysis to [Assignment: organization-defined personnel or roles].

Discussion for Development Process, Standards, and Tools | Automated Vulnerability Analysis (SA-15(7))
Automated tools can be more effective at analyzing exploitable weaknesses or deficiencies in large and complex systems, prioritizing vulnerabilities by severity, and providing recommendations for risk mitigations.

Development Process, Standards, and Tools | Reuse of Threat and Vulnerability Information (SA-15(8))

Description for Development Process, Standards, and Tools | Reuse of Threat and Vulnerability Information (SA-15(8))
Require the developer of the system, system component, or system service to use threat modeling and vulnerability analyses from similar systems, components, or services to inform the current development process.

Discussion for Development Process, Standards, and Tools | Reuse of Threat and Vulnerability Information (SA-15(8))
Analysis of vulnerabilities found in similar software applications can inform potential design and implementation issues for systems under development. Similar systems or system components may exist within developer organizations. Vulnerability information is available from a variety of public and private sector sources, including the NIST National Vulnerability Database.

Component Authenticity | Anti-counterfeit Scanning (SA-19(4))

Description for Component Authenticity | Anti-counterfeit Scanning (SA-19(4))
[Withdrawn: Moved to SR-11(3).]

Discussion for Component Authenticity | Anti-counterfeit Scanning (SA-19(4))

Development Process, Standards, and Tools | Incident Response Plan (SA-15(10))

Description for Development Process, Standards, and Tools | Incident Response Plan (SA-15(10))
Require the developer of the system, system component, or system service to provide, implement, and test an incident response plan.

Discussion for Development Process, Standards, and Tools | Incident Response Plan (SA-15(10))
The incident response plan provided by developers may provide information not readily available to organizations and be incorporated into organizational incident response plans. Developer information may also be extremely helpful, such as when organizations respond to vulnerabilities in commercial off-the-shelf products.

Development Process, Standards, and Tools | Archive System or Component (SA-15(11))

Description for Development Process, Standards, and Tools | Archive System or Component (SA-15(11))
Require the developer of the system or system component to archive the system or component to be released or delivered together with the corresponding evidence supporting the final security and privacy review.

Discussion for Development Process, Standards, and Tools | Archive System or Component (SA-15(11))
Archiving system or system components requires the developer to retain key development artifacts, including hardware specifications, source code, object code, and relevant documentation from the development process that can provide a readily available configuration baseline for system and component upgrades or modifications.

Development Process, Standards, and Tools | Minimize Personally Identifiable Information (SA-15(12))

Description for Development Process, Standards, and Tools | Minimize Personally Identifiable Information (SA-15(12))
Require the developer of the system or system component to minimize the use of personally identifiable information in development and test environments.

Discussion for Development Process, Standards, and Tools | Minimize Personally Identifiable Information (SA-15(12))
Organizations can minimize the risk to an individual's privacy by using techniques such as de-identification or synthetic data. Limiting the use of personally identifiable information in development and test environments helps reduce the level of privacy risk created by a system.

Developer-provided Training (SA-16)

Description for Developer-provided Training (SA-16)
Require the developer of the system, system component, or system service to provide the following training on the correct use and operation of the implemented security and privacy functions, controls, and/or mechanisms: [Assignment: organization-defined training].

Discussion for Developer-provided Training (SA-16)
Developer-provided training applies to external and internal (in-house) developers. Training personnel is essential to ensuring the effectiveness of the controls implemented within organizational systems. Types of training include web-based and computer-based training, classroom-style training, and hands-on training (including micro-training). Organizations can also request training materials from developers to conduct in-house training or offer self-training to organizational personnel. Organizations determine the type of training necessary and may require different types of training for different security and privacy functions, controls, and mechanisms.

Developer Security and Privacy Architecture and Design (SA-17)

Description for Developer Security and Privacy Architecture and Design (SA-17)
Require the developer of the system, system component, or system service to produce a design specification and security and privacy architecture that:
a. Is consistent with the organization's security and privacy architecture that is an integral part the organization's enterprise architecture;
b. Accurately and completely describes the required security and privacy functionality, and the allocation of controls among physical and logical components; and
c. Expresses how individual security and privacy functions, mechanisms, and services work together to provide required security and privacy capabilities and a unified approach to protection.

Discussion for Developer Security and Privacy Architecture and Design (SA-17)
Developer security and privacy architecture and design are directed at external developers, although they could also be applied to internal (in-house) development. In contrast, PL-8 is directed at internal developers to ensure that organizations develop a security and privacy architecture that is integrated with the enterprise architecture. The distinction between SA-17 and PL-8 is especially important when organizations outsource the development of systems, system components, or system services and when there is a requirement to demonstrate consistency with the enterprise architecture and security and privacy architecture of the organization. ISO 15408-2, ISO 15408-3, and SP 800-160-1 provide information on security architecture and design, including formal policy models, security-relevant components, formal and informal correspondence, conceptually simple design, and structuring for least privilege and testing.

Developer Security and Privacy Architecture and Design | Formal Policy Model (SA-17(1))

Description for Developer Security and Privacy Architecture and Design | Formal Policy Model (SA-17(1))
Require the developer of the system, system component, or system service to:
(a) Produce, as an integral part of the development process, a formal policy model describing the [Assignment: organization-defined elements of organizational security and privacy policy] to be enforced; and
(b) Prove that the formal policy model is internally consistent and sufficient to enforce the defined elements of the organizational security and privacy policy when implemented.

Discussion for Developer Security and Privacy Architecture and Design | Formal Policy Model (SA-17(1))
Formal models describe specific behaviors or security and privacy policies using formal languages, thus enabling the correctness of those behaviors and policies to be formally proven. Not all components of systems can be modeled. Generally, formal specifications are scoped to the behaviors or policies of interest, such as nondiscretionary access control policies. Organizations choose the formal modeling language and approach based on the nature of the behaviors and policies to be described and the available tools.

Developer Security and Privacy Architecture and Design | Security-relevant Components (SA-17(2))

Description for Developer Security and Privacy Architecture and Design | Security-relevant Components (SA-17(2))
Require the developer of the system, system component, or system service to:
(a) Define security-relevant hardware, software, and firmware; and
(b) Provide a rationale that the definition for security-relevant hardware, software, and firmware is complete.

Discussion for Developer Security and Privacy Architecture and Design | Security-relevant Components (SA-17(2))
The security-relevant hardware, software, and firmware represent the portion of the system, component, or service that is trusted to perform correctly to maintain required security properties.

Developer Security and Privacy Architecture and Design | Formal Correspondence (SA-17(3))

Description for Developer Security and Privacy Architecture and Design | Formal Correspondence (SA-17(3))
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 in terms of exceptions, error messages, and effects;
(b) Show via proof to the extent feasible with additional informal demonstration as necessary, that the formal top-level specification is consistent with the formal policy model;
(c) Show via informal demonstration, that the formal top-level specification completely covers the interfaces to security-relevant hardware, software, and firmware;
(d) Show that the formal top-level specification is an accurate description of the implemented security-relevant hardware, software, and firmware; and
(e) Describe the security-relevant hardware, software, and firmware mechanisms not addressed in the formal top-level specification but strictly internal to the security-relevant hardware, software, and firmware.

Discussion for Developer Security and Privacy Architecture and Design | Formal Correspondence (SA-17(3))
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 used 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 models 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 on the applicability of formal methods to prove that the specification accurately reflects the implementation. Hardware, software, and firmware mechanisms internal to security-relevant components include mapping registers and direct memory input and output.

Developer Security and Privacy Architecture and Design | Informal Correspondence (SA-17(4))

Description for Developer Security and Privacy Architecture and Design | Informal Correspondence (SA-17(4))
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 [Selection: informal demonstration; convincing argument with formal methods as feasible] that the descriptive top-level specification is consistent with the formal policy model;
(c) Show via informal demonstration, that the descriptive top-level specification completely covers the interfaces to security-relevant hardware, software, and firmware;
(d) Show that the descriptive top-level specification is an accurate description of the interfaces to security-relevant hardware, software, and firmware; and
(e) Describe the security-relevant hardware, software, and firmware mechanisms not addressed in the descriptive top-level specification but strictly internal to the security-relevant hardware, software, and firmware.

Discussion for Developer Security and Privacy Architecture and Design | Informal Correspondence (SA-17(4))
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 additional code or implementation detail has no impact on the behaviors or policies being modeled. 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 show such consistency. Hardware, software, and firmware mechanisms strictly internal to security-relevant hardware, software, and firmware include mapping registers and direct memory input and output.

Developer Security and Privacy Architecture and Design | Conceptually Simple Design (SA-17(5))

Description for Developer Security and Privacy Architecture and Design | Conceptually Simple Design (SA-17(5))
Require the developer of the system, system component, or system service to:
(a) Design and structure the security-relevant hardware, software, and firmware to use a complete, conceptually simple protection mechanism with precisely defined semantics; and
(b) Internally structure the security-relevant hardware, software, and firmware with specific regard for this mechanism.

Discussion for Developer Security and Privacy Architecture and Design | Conceptually Simple Design (SA-17(5))
The principle of reduced complexity states that the system design is as simple and small as possible (see SA-8(7)). A small and simple design is easier to understand and analyze and is also less prone to error (see AC-25, SA-8(13)). The principle of reduced complexity applies to any aspect of a system, but it has particular importance for security due to the various analyses performed to obtain evidence about the emergent security property of the system. For such analyses 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 and facilitates the 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. That is, simpler systems contain fewer vulnerabilities. An important benefit of reduced complexity is that it is easier to understand whether the 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 any such conclusion about correctness, completeness, and existence of vulnerabilities can be reached with a higher degree of assurance in contrast to conclusions reached in situations where the system design is inherently more complex.

Developer Security and Privacy Architecture and Design | Structure for Testing (SA-17(6))

Description for Developer Security and Privacy Architecture and Design | Structure for Testing (SA-17(6))
Require the developer of the system, system component, or system service to structure security-relevant hardware, software, and firmware to facilitate testing.

Discussion for Developer Security and Privacy Architecture and Design | Structure for Testing (SA-17(6))
Applying the security design principles in SP 800-160-1 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 trustworthiness of the system, system component, or service.

Developer Security and Privacy Architecture and Design | Structure for Least Privilege (SA-17(7))

Description for Developer Security and Privacy Architecture and Design | Structure for Least Privilege (SA-17(7))
Require the developer of the system, system component, or system service to structure security-relevant hardware, software, and firmware to facilitate controlling access with least privilege.

Discussion for Developer Security and Privacy Architecture and Design | Structure for Least Privilege (SA-17(7))
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 secure system design. Interfaces used to invoke component capability are available to only certain subsets of the user population, and component design supports a sufficiently fine granularity of privilege decomposition. For example, in the case of an audit mechanism, there may be an interface for the audit manager, who configures the audit settings; an interface for the audit operator, who ensures that audit data is safely collected and stored; and, finally, yet another interface for the audit reviewer, who only has a need to view the audit data that has been collected but no need to perform operations on that data.
In addition to its manifestations at the system interface, least privilege can be used as a guiding principle for the internal structure of the system itself. One aspect of internal least privilege is to construct modules so that only the elements encapsulated by the module are directly operated upon by the functions 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 internal least privilege is that the scope of a given module or component includes only those system elements that are necessary for its functionality, and the access modes to the elements (e.g., read, write) are minimal.

Developer Security and Privacy Architecture and Design | Orchestration (SA-17(8))

Description for Developer Security and Privacy Architecture and Design | Orchestration (SA-17(8))
Design [Assignment: organization-defined critical systems or system components] with coordinated behavior to implement the following capabilities: [Assignment: organization-defined capabilities, by system or component].

Discussion for Developer Security and Privacy Architecture and Design | Orchestration (SA-17(8))
Security resources that are distributed, located at different layers or in different system elements, or are implemented to support different aspects of trustworthiness can interact in unforeseen or incorrect ways. Adverse consequences can include cascading failures, interference, or coverage gaps. Coordination of the behavior of security resources (e.g., by ensuring that one patch is installed across all resources before making a configuration change that assumes that the patch is propagated) can avert such negative interactions.

Developer Security and Privacy Architecture and Design | Design Diversity (SA-17(9))

Description for Developer Security and Privacy Architecture and Design | Design Diversity (SA-17(9))
Use different designs for [Assignment: organization-defined critical systems or system components] to satisfy a common set of requirements or to provide equivalent functionality.

Discussion for Developer Security and Privacy Architecture and Design | Design Diversity (SA-17(9))
Design diversity is achieved by supplying the same requirements specification to multiple developers, each of whom is responsible for developing a variant of the system or system component that meets the requirements. Variants can be in software design, in hardware design, or in both hardware and a software design. Differences in the designs of the variants can result from developer experience (e.g., prior use of a design pattern), design style (e.g., when decomposing a required function into smaller tasks, determining what constitutes a separate task and how far to decompose tasks into sub-tasks), selection of libraries to incorporate into the variant, and the development environment (e.g., different design tools make some design patterns easier to visualize). Hardware design diversity includes making different decisions about what information to keep in analog form and what information to convert to digital form, transmitting the same information at different times, and introducing delays in sampling (temporal diversity). Design diversity is commonly used to support fault tolerance.

Developer Screening | Validation of Screening (SA-21(1))

Description for Developer Screening | Validation of Screening (SA-21(1))
[Withdrawn: Incorporated into SA-21.]

Discussion for Developer Screening | Validation of Screening (SA-21(1))

Unsupported System Components | Alternative Sources for Continued Support (SA-22(1))

Description for Unsupported System Components | Alternative Sources for Continued Support (SA-22(1))
[Withdrawn: Incorporated into SA-22.]

Discussion for Unsupported System Components | Alternative Sources for Continued Support (SA-22(1))

Acquisition Process | Assignment of Components to Systems (SA-4(4))

Description for Acquisition Process | Assignment of Components to Systems (SA-4(4))
[Withdrawn: Incorporated into CM-8(9).]

Discussion for Acquisition Process | Assignment of Components to Systems (SA-4(4))

System Documentation | Functional Properties of Security Controls (SA-5(1))

Description for System Documentation | Functional Properties of Security Controls (SA-5(1))
[Withdrawn: Incorporated into SA-4(1).]

Discussion for System Documentation | Functional Properties of Security Controls (SA-5(1))

System Documentation | Security-relevant External System Interfaces (SA-5(2))

Description for System Documentation | Security-relevant External System Interfaces (SA-5(2))
[Withdrawn: Incorporated into SA-4(2).]

Discussion for System Documentation | Security-relevant External System Interfaces (SA-5(2))

System Documentation | High-level Design (SA-5(3))

Description for System Documentation | High-level Design (SA-5(3))
[Withdrawn: Incorporated into SA-4(2).]

Discussion for System Documentation | High-level Design (SA-5(3))

System Documentation | Low-level Design (SA-5(4))

Description for System Documentation | Low-level Design (SA-5(4))
[Withdrawn: Incorporated into SA-4(2).]

Discussion for System Documentation | Low-level Design (SA-5(4))

System Documentation | Source Code (SA-5(5))

Description for System Documentation | Source Code (SA-5(5))
[Withdrawn: Incorporated into SA-4(2).]

Discussion for System Documentation | Source Code (SA-5(5))

Customized Development of Critical Components (SA-20)

Description for Customized Development of Critical Components (SA-20)
Reimplement or custom develop the following critical system components: [Assignment: organization-defined critical system components].

Discussion for Customized Development of Critical Components (SA-20)
Organizations determine that certain system components likely cannot be trusted due to specific threats to and vulnerabilities in those components for which there are no viable security controls to adequately mitigate risk. Reimplementation or custom development of such components may satisfy requirements for higher assurance and is carried out by initiating changes to system components (including hardware, software, and firmware) such that the standard attacks by adversaries are less likely to succeed. In situations where no alternative sourcing is available and organizations choose not to reimplement or custom develop critical system components, additional controls can be employed. Controls include enhanced auditing, restrictions on source code and system utility access, and protection from deletion of system and application files.

Developer Screening (SA-21)

Description for Developer Screening (SA-21)
Require that the developer of [Assignment: organization-defined system, system component, or system service]:
a. Has appropriate access authorizations as determined by assigned [Assignment: organization-defined official government duties]; and
b. Satisfies the following additional personnel screening criteria: [Assignment: organization-defined additional personnel screening criteria].

Discussion for Developer Screening (SA-21)
Developer screening is directed at external developers. Internal developer screening is addressed by PS-3. Because the system, system component, or system service may be used in critical activities essential to the national or economic security interests of the United States, organizations have a strong interest in ensuring that developers are trustworthy. The degree of trust required of developers may need to be consistent with that of the individuals who access the systems, system components, or system services once deployed. Authorization and personnel screening criteria include clearances, background checks, citizenship, and nationality. Developer trustworthiness may also include a review and analysis of company ownership and relationships that the company has with entities that may potentially affect the quality and reliability of the systems, components, or services being developed. Satisfying the required access authorizations and personnel screening criteria includes providing a list of all individuals who are authorized to perform development activities on the selected system, system component, or system service so that organizations can validate that the developer has satisfied the authorization and screening requirements.

Software Usage Restrictions (SA-6)

Description for Software Usage Restrictions (SA-6)
[Withdrawn: Incorporated into CM-10 and SI-7.]

Discussion for Software Usage Restrictions (SA-6)

Unsupported System Components (SA-22)

Description for Unsupported System Components (SA-22)
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 providers]].

Discussion for Unsupported System Components (SA-22)
Support for system components includes software patches, firmware updates, replacement parts, and maintenance contracts. An example of unsupported components includes when vendors no longer provide critical software patches or product updates, which can result in an opportunity for adversaries to exploit weaknesses in the installed components. Exceptions to replacing unsupported system components include systems that provide critical mission or business capabilities 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 manufacturers, developers, or vendors when such components remain essential to organizational

mission and business functions. 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 provide ongoing support for the designated unsupported components through contractual relationships. Such contractual relationships can include open-source software value-added vendors. The increased risk of using unsupported system components can be mitigated, for example, by prohibiting the connection of such components to public or uncontrolled networks, or implementing other forms of isolation.

User-installed Software (SA-7)

Description for User-installed Software (SA-7)
[Withdrawn: Incorporated into CM-11 and SI-7.]

Discussion for User-installed Software (SA-7)

Specialization (SA-23)

Description for Specialization (SA-23)
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.

Discussion for Specialization (SA-23)
It is often necessary for a system or system component that supports mission-essential services or functions to be enhanced to maximize the trustworthiness of the resource. 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 on the organization-defined resources.

Policy and Procedures (SC-1)

Description for Policy and Procedures (SC-1)
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] system and communications protection policy that:
(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection controls;
b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and communications protection policy and procedures; and
c. Review and update the current system and communications protection:
1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

Discussion for Policy and Procedures (SC-1)
System and communications protection policy and procedures address the controls in the SC family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of system and communications protection policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, 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. Events that may precipitate an update to system and communications protection policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Separation of System and User Functionality (SC-2)

Description for Separation of System and User Functionality (SC-2)
Separate user functionality, including user interface services, from system management functionality.

Discussion for Separation of System and User Functionality (SC-2)
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 may separate system management functions from user functions 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 web administrative interfaces that employ separate authentication methods for users of any other system resources. Separation of system and user functions may include isolating administrative interfaces on different domains and with additional access controls. The separation of system and user functionality can be achieved by applying the systems security engineering design principles in SA-8, including SA-8(1), SA-8(3), SA-8(4), SA-8(10), SA-8(12), SA-8(13), SA-8(14), and SA-8(18).

Separation of System and User Functionality | Interfaces for Non-privileged Users (SC-2(1))

Description for Separation of System and User Functionality | Interfaces for Non-privileged Users (SC-2(1))
Prevent the presentation of system management functionality at interfaces to non-privileged users.

Discussion for Separation of System and User Functionality | Interfaces for Non-privileged Users (SC-2(1))
Preventing the presentation of system management functionality at interfaces to non-privileged users ensures that system administration options, including administrator privileges, are not available to the general user population. Restricting user access also prohibits the use of the grey-out option commonly used to eliminate accessibility to such information. One potential solution is to withhold system administration options until users establish sessions with administrator privileges.

Separation of System and User Functionality | Disassociability (SC-2(2))

Description for Separation of System and User Functionality | Disassociability (SC-2(2))
Store state information from applications and software separately.

Discussion for Separation of System and User Functionality | Disassociability (SC-2(2))
If a system is compromised, storing applications and software separately from state information about users' interactions with an application may better protect individuals' privacy.

Security Function Isolation (SC-3)

Description for Security Function Isolation (SC-3)
Isolate security functions from nonsecurity functions.

Discussion for Security Function Isolation (SC-3)
Security functions are isolated from nonsecurity functions by means of an isolation boundary implemented within a system via partitions and domains. The isolation boundary controls access to and protects the integrity of the hardware, software, and firmware that perform system security functions. Systems implement code separation in many ways, such as through the provision of security kernels via processor rings or processor modes. For non-kernel code, security function isolation is often achieved through file system protections that protect the code on disk and address space protections that protect executing code. Systems can restrict access to security functions using access control mechanisms and by implementing least privilege capabilities. While the ideal is for all code within the defined security function isolation boundary to only contain security-relevant code, it is sometimes necessary to include nonsecurity functions as an exception. The isolation of security functions from nonsecurity functions can be achieved by applying the systems security engineering design principles in SA-8, including SA-8(1), SA-8(3), SA-8(4), SA-8(10), SA-8(12), SA-8(13), SA-8(14), and SA-8(18).

Security Function Isolation | Hardware Separation (SC-3(1))

Description for Security Function Isolation | Hardware Separation (SC-3(1))
Employ hardware separation mechanisms to implement security function isolation.

Discussion for Security Function Isolation | Hardware Separation (SC-3(1))
Hardware separation mechanisms include hardware ring architectures that are implemented within microprocessors and hardware-enforced address segmentation used to support logically distinct storage objects with separate attributes (i.e., readable, writeable).

Security Function Isolation | Access and Flow Control Functions (SC-3(2))

Description for Security Function Isolation | Access and Flow Control Functions (SC-3(2))
Isolate security functions enforcing access and information flow control from nonsecurity functions and from other security functions.

Discussion for Security Function Isolation | Access and Flow Control Functions (SC-3(2))
Security function isolation occurs because of implementation. The functions can still be scanned and monitored. Security functions that are potentially isolated from access and flow control enforcement functions include auditing, intrusion detection, and malicious code protection functions.

Security Function Isolation | Minimize Nonsecurity Functionality (SC-3(3))

Description for Security Function Isolation | Minimize Nonsecurity Functionality (SC-3(3))
Minimize the number of nonsecurity functions included within the isolation boundary containing security functions.

Discussion for Security Function Isolation | Minimize Nonsecurity Functionality (SC-3(3))
Where it is not feasible to achieve strict isolation of nonsecurity functions from security functions, it is necessary to take actions to minimize nonsecurity-relevant functions within the security function boundary. Nonsecurity functions contained within the isolation boundary are considered security-relevant because errors or malicious code in the software can directly impact the security functions of systems. The fundamental design objective is that the specific portions of systems that provide information security are of minimal size and complexity. Minimizing the number of nonsecurity 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 minimizing the nonsecurity functions within the isolation boundaries, the amount of code that is trusted to enforce security policies is significantly reduced, thus contributing to understandability.

Security Function Isolation | Module Coupling and Cohesiveness (SC-3(4))

Description for Security Function Isolation | Module Coupling and Cohesiveness (SC-3(4))
Implement security functions as largely independent modules that maximize internal cohesiveness within modules and minimize coupling between modules.

Discussion for Security Function Isolation | Module Coupling and Cohesiveness (SC-3(4))
The reduction of inter-module interactions helps to constrain 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 other modules. Cohesion refers to the relationship between functions within a module. Best practices in software engineering and systems security engineering rely on layering, minimization, and modular decomposition to reduce and manage complexity. This produces software modules that are highly cohesive and loosely coupled.

Security Function Isolation | Layered Structures (SC-3(5))

Description for Security Function Isolation | Layered Structures (SC-3(5))
Implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.

Discussion for Security Function Isolation | Layered Structures (SC-3(5))
The implementation of layered structures with minimized interactions among security functions and non-looping layers (i.e., lower-layer functions do not depend on higher-layer functions) enables the isolation of security functions and the management of complexity.

Information in Shared System Resources (SC-4)

Description for Information in Shared System Resources (SC-4)
Prevent unauthorized and unintended information transfer via shared system resources.

Discussion for Information in Shared System Resources (SC-4)
Preventing unauthorized and unintended information transfer via shared system resources stops information produced by the actions of prior users or roles (or the actions of processes acting on behalf of prior users or roles) from being available to current users or roles (or current processes acting on behalf of current users or roles) that obtain access to shared system resources after those resources have been released back to the system. Information in shared system resources also applies to encrypted representations of information. In other contexts, control of information in shared system resources is referred to as object reuse and residual information protection. Information in shared system resources does not address information remanence, which refers to the residual representation of data that has been nominally deleted; covert channels (including storage and timing channels), where shared system resources are manipulated to violate information flow restrictions; or components within systems for which there are only single users or roles.

Cryptographic Key Establishment and Management | PKI Certificates (SC-12(4))

Description for Cryptographic Key Establishment and Management | PKI Certificates (SC-12(4))
[Withdrawn: Incorporated into SC-12(3).]

Discussion for Cryptographic Key Establishment and Management | PKI Certificates (SC-12(4))

Information in Shared System Resources | Multilevel or Periods Processing (SC-4(2))

Description for Information in Shared System Resources | Multilevel or Periods Processing (SC-4(2))
Prevent unauthorized information transfer via shared resources in accordance with [Assignment: organization-defined procedures] when system processing explicitly switches between different information classification levels or security categories.

Discussion for Information in Shared System Resources | Multilevel or Periods Processing (SC-4(2))
Changes in processing levels can occur during multilevel or periods processing with information at different classification levels or security categories. It can also occur during serial reuse of hardware components at different classification levels. Organization-defined procedures can include approved sanitization processes for electronically stored information.

Denial-of-service Protection (SC-5)

Description for Denial-of-service Protection (SC-5)
a. [Selection: Protect against; Limit] the effects of the following types of denial-of-service events: [Assignment: organization-defined types of denial-of-service events]; and
b. Employ the following controls to achieve the denial-of-service objective: [Assignment: organization-defined controls by type of denial-of-service event].

Discussion for Denial-of-service Protection (SC-5)
Denial-of-service events may occur due to a variety of internal and external causes, such as an attack by an adversary or a lack of planning to support organizational needs with respect to capacity and bandwidth. Such attacks can occur across a wide range of network protocols (e.g., IPv4, IPv6). A variety of technologies are available to limit or eliminate the origination and effects of denial-of-service events. For example, boundary protection devices can filter certain types of packets to protect system components on internal networks from being directly affected by or the source of denial-of-service attacks. Employing increased network capacity and bandwidth combined with service redundancy also reduces the susceptibility to denial-of-service events.

Denial-of-service Protection | Restrict Ability to Attack Other Systems (SC-5(1))

Description for Denial-of-service Protection | Restrict Ability to Attack Other Systems (SC-5(1))
Restrict the ability of individuals to launch the following denial-of-service attacks against other systems: [Assignment: organization-defined denial-of-service attacks].

Discussion for Denial-of-service Protection | Restrict Ability to Attack Other Systems (SC-5(1))
Restricting the ability of individuals to launch denial-of-service attacks requires the mechanisms commonly used for such attacks to be unavailable. Individuals of concern include hostile insiders or external adversaries who have breached or compromised the system and are using it to launch a denial-of-service attack. Organizations can restrict the ability of individuals to connect and transmit arbitrary information on the transport medium (i.e., wired networks, wireless networks, spoofed Internet protocol packets). Organizations can also limit the ability of individuals to use excessive system resources. Protection against individuals having the ability to launch denial-of-service attacks may be implemented on specific systems or boundary devices that prohibit egress to potential target systems.

Denial-of-service Protection | Capacity, Bandwidth, and Redundancy (SC-5(2))

Description for Denial-of-service Protection | Capacity, Bandwidth, and Redundancy (SC-5(2))
Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding denial-of-service attacks.

Discussion for Denial-of-service Protection | Capacity, Bandwidth, and Redundancy (SC-5(2))
Managing capacity ensures that sufficient capacity is available to counter flooding attacks. Managing capacity includes establishing selected usage priorities, quotas, partitioning, or load balancing.

Denial-of-service Protection | Detection and Monitoring (SC-5(3))

Description for Denial-of-service Protection | Detection and Monitoring (SC-5(3))
(a) Employ the following monitoring tools to detect indicators of denial-of-service attacks against, or launched from, the system: [Assignment: organization-defined monitoring tools]; and
(b) Monitor the following system resources to determine if sufficient resources exist to prevent effective denial-of-service attacks: [Assignment: organization-defined system resources].

Discussion for Denial-of-service Protection | Detection and Monitoring (SC-5(3))
Organizations consider the utilization and capacity of system resources when managing risk associated with a denial of service due to malicious attacks. Denial-of-service attacks can originate from external or internal sources. System resources that are sensitive to denial of service include physical disk storage, memory, and CPU cycles. Techniques used to prevent denial-of-service attacks related to storage utilization and capacity include instituting disk quotas, configuring systems to automatically alert administrators when specific storage capacity thresholds are reached, using file compression technologies to maximize available storage space, and imposing separate partitions for system and user data.

Resource Availability (SC-6)

Description for Resource Availability (SC-6)
Protect the availability of resources by allocating [Assignment: organization-defined resources] by [Selection (one or more): priority; quota; [Assignment: organization-defined controls]].

Discussion for Resource Availability (SC-6)
Priority protection prevents lower-priority processes from delaying or interfering with the system that services higher-priority processes. Quotas prevent users or processes from obtaining more than predetermined amounts of resources.

Boundary Protection (SC-7)

Description for Boundary Protection (SC-7)
a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system;
b. Implement subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and
c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.

Discussion for Boundary Protection (SC-7)
Managed interfaces include gateways, routers, firewalls, guards, network-based malicious code analysis, virtualization 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 or DMZs. Restricting or prohibiting interfaces 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. SP 800-189 provides additional information on source address validation techniques to prevent ingress and egress of traffic with spoofed addresses. Commercial telecommunications 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. Boundary protection may be implemented as a common control for all or part of an organizational network such that the boundary to be protected is greater than a system-specific boundary (i.e., an authorization boundary).

Cryptographic Key Establishment and Management | PKI Certificates / Hardware Tokens (SC-12(5))

Description for Cryptographic Key Establishment and Management | PKI Certificates / Hardware Tokens (SC-12(5))
[Withdrawn: Incorporated into SC-12(3).]

Discussion for Cryptographic Key Establishment and Management | PKI Certificates / Hardware Tokens (SC-12(5))

Cryptographic Protection | FIPS-validated Cryptography (SC-13(1))

Description for Cryptographic Protection | FIPS-validated Cryptography (SC-13(1))
[Withdrawn: Incorporated into SC-13.]

Discussion for Cryptographic Protection | FIPS-validated Cryptography (SC-13(1))

Boundary Protection | Access Points (SC-7(3))

Description for Boundary Protection | Access Points (SC-7(3))
Limit the number of external network connections to the system.

Discussion for Boundary Protection | Access Points (SC-7(3))
Limiting the number of external network connections facilitates monitoring of inbound and outbound communications traffic. The Trusted Internet Connection DHS TIC initiative is an example of a federal guideline that requires limits on the number of external network connections. Limiting the number of external network connections to the system is important during transition periods from older to newer technologies (e.g., transitioning from IPv4 to IPv6 network protocols). Such transitions may require implementing the older and newer technologies simultaneously during the transition period and thus increase the number of access points to the system.

Boundary Protection | External Telecommunications Services (SC-7(4))

Description for Boundary Protection | External Telecommunications Services (SC-7(4))
(a) Implement a managed interface for each external telecommunication service;
(b) Establish a traffic flow policy for each managed interface;
(c) Protect the confidentiality and integrity of the information being transmitted across each interface;
(d) Document each exception to the traffic flow policy with a supporting mission or business need and duration of that need;
(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;
(f) Prevent unauthorized exchange of control plane traffic with external networks;
(g) Publish information to enable remote networks to detect unauthorized control plane traffic from internal networks; and
(h) Filter unauthorized control plane traffic from external networks.

Discussion for Boundary Protection | External Telecommunications Services (SC-7(4))
External telecommunications services can provide data and/or voice communications services. Examples of control plane traffic include Border Gateway Protocol (BGP) routing, Domain Name System (DNS), and management protocols. See SP 800-189 for additional information on the use of the resource public key infrastructure (RPKI) to protect BGP routes and detect unauthorized BGP announcements.

Boundary Protection | Deny by Default — Allow by Exception (SC-7(5))

Description for Boundary Protection | Deny by Default — Allow by Exception (SC-7(5))
Deny network communications traffic by default and allow network communications traffic by exception [Selection (one or more): at managed interfaces; for [Assignment: organization-defined systems]].

Discussion for Boundary Protection | Deny by Default — Allow by Exception (SC-7(5))
Denying by default and allowing by exception applies to inbound and outbound network communications traffic. A deny-all, permit-by-exception network communications traffic policy ensures that only those system connections that are essential and approved are allowed. Deny by default, allow by exception also applies to a system that is connected to an external system.

Cryptographic Protection | NSA-approved Cryptography (SC-13(2))

Description for Cryptographic Protection | NSA-approved Cryptography (SC-13(2))
[Withdrawn: Incorporated into SC-13.]

Discussion for Cryptographic Protection | NSA-approved Cryptography (SC-13(2))

Boundary Protection | Split Tunneling for Remote Devices (SC-7(7))

Description for Boundary Protection | Split Tunneling for Remote Devices (SC-7(7))
Prevent split tunneling for remote devices connecting to organizational systems unless the split tunnel is securely provisioned using [Assignment: organization-defined safeguards].

Discussion for Boundary Protection | Split Tunneling for Remote Devices (SC-7(7))
Split tunneling is the process of allowing a remote user or device to establish a non-remote connection with a system and simultaneously communicate via some other connection to a resource in an external network. This method of network access enables a user to access remote devices and simultaneously, access uncontrolled networks. 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 to exfiltration of organizational information. Split tunneling can be prevented by disabling configuration settings that allow such capability in remote devices and by preventing those configuration settings from being configurable by users. Prevention can also be achieved by the detection of split tunneling (or of configuration settings that allow split tunneling) in the remote device, and by prohibiting the connection if the remote device is using split tunneling. A virtual private network (VPN) can be used to securely provision a split tunnel. A securely provisioned VPN includes locking connectivity to exclusive, managed, and named environments, or to a specific set of pre-approved addresses, without user control.

Boundary Protection | Route Traffic to Authenticated Proxy Servers (SC-7(8))

Description for Boundary Protection | Route Traffic to Authenticated Proxy Servers (SC-7(8))
Route [Assignment: organization-defined internal communications traffic] to [Assignment: organization-defined external networks] through authenticated proxy servers at managed interfaces.

Discussion for Boundary Protection | Route Traffic to Authenticated Proxy Servers (SC-7(8))
External networks are networks outside of organizational control. A proxy server is a server (i.e., system or application) that acts as an intermediary for clients requesting system resources from non-organizational or other organizational servers. System resources that may be requested include files, connections, web pages, or services. Client requests established through a connection to a proxy server are assessed to manage complexity and provide additional protection by limiting direct connectivity. Web content filtering devices are one of the most common proxy servers that provide access to the Internet. Proxy servers can support the logging of Transmission Control Protocol sessions and the blocking of specific Uniform Resource Locators, Internet Protocol addresses, and domain names. Web proxies can be configured with organization-defined lists of authorized and unauthorized websites. Note that proxy servers may inhibit the use of virtual private networks (VPNs) and create the potential for man-in-the-middle attacks (depending on the implementation).

Boundary Protection | Restrict Threatening Outgoing Communications Traffic (SC-7(9))

Description for Boundary Protection | Restrict Threatening Outgoing Communications Traffic (SC-7(9))
(a) Detect and deny outgoing communications traffic posing a threat to external systems; and
(b) Audit the identity of internal users associated with denied communications.

Discussion for Boundary Protection | Restrict Threatening Outgoing Communications Traffic (SC-7(9))
Detecting outgoing communications traffic from internal actions that may pose threats to external systems is known as extrusion detection. Extrusion detection is carried out within the system at managed interfaces. Extrusion detection includes the analysis of incoming and outgoing communications traffic while searching for indications of internal threats to the security of external systems. Internal threats to external systems include traffic indicative of denial-of-service attacks, traffic with spoofed source addresses, and traffic that contains malicious code. Organizations have criteria to determine, update, and manage identified threats related to extrusion detection.

Boundary Protection | Prevent Exfiltration (SC-7(10))

Description for Boundary Protection | Prevent Exfiltration (SC-7(10))
(a) Prevent the exfiltration of information; and
(b) Conduct exfiltration tests [Assignment: organization-defined frequency].

Discussion for Boundary Protection | Prevent Exfiltration (SC-7(10))
Prevention of exfiltration applies to both the intentional and unintentional exfiltration of information. Techniques used to prevent the exfiltration of information from systems may be implemented at internal endpoints, external boundaries, and across managed interfaces and include adherence to protocol formats, monitoring for beaconing activity from systems, disconnecting external network interfaces except when explicitly needed, employing traffic profile analysis to detect deviations from the volume and types of traffic expected, call backs to command and control centers, conducting penetration testing, monitoring for steganography, disassembling and reassembling packet headers, and using data loss and data leakage prevention tools. Devices that enforce strict adherence to protocol formats include deep packet inspection firewalls and Extensible Markup Language (XML) gateways. The devices verify adherence to protocol formats and specifications at the application layer and identify vulnerabilities that cannot be detected by devices that operate at the network or transport layers. The prevention of exfiltration is similar to data loss prevention or data leakage prevention and is closely associated with cross-domain solutions and system guards that enforce information flow requirements.

Boundary Protection | Restrict Incoming Communications Traffic (SC-7(11))

Description for Boundary Protection | Restrict Incoming Communications Traffic (SC-7(11))
Only allow incoming communications from [Assignment: organization-defined authorized sources] to be routed to [Assignment: organization-defined authorized destinations].

Discussion for Boundary Protection | Restrict Incoming Communications Traffic (SC-7(11))
General source address validation techniques are applied to restrict the use of illegal and unallocated source addresses as well as source addresses that should only be used within the system. The restriction of incoming communications traffic provides determinations that source and destination address pairs represent authorized or allowed communications. Determinations can be based on several factors, including the presence of such address pairs in the lists of authorized or allowed communications, the absence of such address pairs in lists of unauthorized or disallowed pairs, or meeting more general rules for authorized or allowed source and destination pairs. Strong 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.

Boundary Protection | Host-based Protection (SC-7(12))

Description for Boundary Protection | Host-based Protection (SC-7(12))
Implement [Assignment: organization-defined host-based boundary protection mechanisms] at [Assignment: organization-defined system components].

Discussion for Boundary Protection | Host-based Protection (SC-7(12))
Host-based boundary protection mechanisms include host-based firewalls. System components that employ host-based boundary protection mechanisms include servers, workstations, notebook computers, and mobile devices.

Boundary Protection | Isolation of Security Tools, Mechanisms, and Support Components (SC-7(13))

Description for Boundary Protection | Isolation of Security Tools, Mechanisms, and Support Components (SC-7(13))
Isolate [Assignment: organization-defined information security tools, mechanisms, and support components] from other internal system components by implementing physically separate subnetworks with managed interfaces to other components of the system.

Discussion for Boundary Protection | Isolation of Security Tools, Mechanisms, and Support Components (SC-7(13))
Physically separate subnetworks with managed interfaces are useful in isolating computer network defenses from critical operational processing networks to prevent adversaries from discovering the analysis and forensics techniques employed by organizations.

Boundary Protection | Protect Against Unauthorized Physical Connections (SC-7(14))

Description for Boundary Protection | Protect Against Unauthorized Physical Connections (SC-7(14))
Protect against unauthorized physical connections at [Assignment: organization-defined managed interfaces].

Discussion for Boundary Protection | Protect Against Unauthorized Physical Connections (SC-7(14))
Systems that operate at different security categories or classification levels may share common physical and environmental controls, since the systems may share space within the same facilities. In practice, it is possible that these separate systems may share common equipment rooms, wiring closets, and cable distribution paths. Protection against unauthorized physical connections can be achieved by using clearly identified and physically separated cable trays, connection frames, and patch panels for each side of managed interfaces with physical access controls that enforce limited authorized access to these items.

Boundary Protection | Networked Privileged Accesses (SC-7(15))

Description for Boundary Protection | Networked Privileged Accesses (SC-7(15))
Route networked, privileged accesses through a dedicated, managed interface for purposes of access control and auditing.

Discussion for Boundary Protection | Networked Privileged Accesses (SC-7(15))
Privileged access provides greater accessibility to system functions, including security functions. Adversaries attempt to gain privileged access to systems through remote access to cause adverse mission or business impacts, such as by exfiltrating information or bringing down a critical system capability. Routing networked, privileged access requests through a dedicated, managed interface further restricts privileged access for increased access control and auditing.

Boundary Protection | Prevent Discovery of System Components (SC-7(16))

Description for Boundary Protection | Prevent Discovery of System Components (SC-7(16))
Prevent the discovery of specific system components that represent a managed interface.

Discussion for Boundary Protection | Prevent Discovery of System Components (SC-7(16))
Preventing the discovery of system components representing a managed interface helps protect network addresses of those components from discovery through common tools and techniques used to identify devices on networks. Network addresses are not available for discovery and require prior knowledge for access. Preventing the 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.

Boundary Protection | Automated Enforcement of Protocol Formats (SC-7(17))

Description for Boundary Protection | Automated Enforcement of Protocol Formats (SC-7(17))
Enforce adherence to protocol formats.

Discussion for Boundary Protection | Automated Enforcement of Protocol Formats (SC-7(17))
System components that enforce protocol formats include deep packet inspection firewalls and XML gateways. The components 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 layers.

Boundary Protection | Fail Secure (SC-7(18))

Description for Boundary Protection | Fail Secure (SC-7(18))
Prevent systems from entering unsecure states in the event of an operational failure of a boundary protection device.

Discussion for Boundary Protection | Fail Secure (SC-7(18))
Fail secure is a condition achieved by employing mechanisms to ensure that in the event of operational failures of boundary protection devices at managed interfaces, systems do not enter into unsecure states where intended security properties no longer hold. Managed interfaces include routers, firewalls, and application gateways that reside on protected subnetworks (commonly referred to as demilitarized zones). Failures of boundary protection devices cannot lead to or cause information external to the devices to enter the devices nor can failures permit unauthorized information releases.

Boundary Protection | Block Communication from Non-organizationally Configured Hosts (SC-7(19))

Description for Boundary Protection | Block Communication from Non-organizationally Configured Hosts (SC-7(19))
Block inbound and outbound communications traffic between [Assignment: organization-defined communication clients] that are independently configured by end users and external service providers.

Discussion for Boundary Protection | Block Communication from Non-organizationally Configured Hosts (SC-7(19))
Communication clients independently configured by end users and external service providers include instant messaging clients and video conferencing software and applications. Traffic blocking does not apply to communication clients that are configured by organizations to perform authorized functions.

Boundary Protection | Dynamic Isolation and Segregation (SC-7(20))

Description for Boundary Protection | Dynamic Isolation and Segregation (SC-7(20))
Provide the capability to dynamically isolate [Assignment: organization-defined system components] from other system components.

Discussion for Boundary Protection | Dynamic Isolation and Segregation (SC-7(20))
The capability to dynamically isolate certain internal system components is useful when it is necessary to partition or separate system components of questionable origin from components that possess greater trustworthiness. 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.

Boundary Protection | Isolation of System Components (SC-7(21))

Description for Boundary Protection | Isolation of System Components (SC-7(21))
Employ boundary protection mechanisms to isolate [Assignment: organization-defined system components] supporting [Assignment: organization-defined missions and/or business functions].

Discussion for Boundary Protection | Isolation of System Components (SC-7(21))
Organizations can isolate system components that perform different mission or business functions. Such isolation limits unauthorized information flows among system components and provides the opportunity to deploy greater levels of protection for selected system components. Isolating system components with boundary protection mechanisms provides the capability for increased protection of individual system components and to more effectively control information flows between those components. Isolating system components provides enhanced protection that limits the potential harm from hostile cyber-attacks and errors. The degree of isolation varies depending upon the mechanisms chosen. Boundary protection mechanisms include routers, gateways, and firewalls that separate system components into physically separate networks or subnetworks; cross-domain devices that separate subnetworks; virtualization techniques; and the encryption of information flows among system components using distinct encryption keys.

Boundary Protection | Separate Subnets for Connecting to Different Security Domains (SC-7(22))

Description for Boundary Protection | Separate Subnets for Connecting to Different Security Domains (SC-7(22))
Implement separate network addresses to connect to systems in different security domains.

Discussion for Boundary Protection | Separate Subnets for Connecting to Different Security Domains (SC-7(22))
The decomposition of systems into subnetworks (i.e., subnets) helps to provide the appropriate level of protection for network connections to different security domains that contain information with different security categories or classification levels.

Boundary Protection | Disable Sender Feedback on Protocol Validation Failure (SC-7(23))

Description for Boundary Protection | Disable Sender Feedback on Protocol Validation Failure (SC-7(23))
Disable feedback to senders on protocol format validation failure.

Discussion for Boundary Protection | Disable Sender Feedback on Protocol Validation Failure (SC-7(23))
Disabling feedback to senders when there is a failure in protocol validation format prevents adversaries from obtaining information that would otherwise be unavailable.

Boundary Protection | Personally Identifiable Information (SC-7(24))

Description for Boundary Protection | Personally Identifiable Information (SC-7(24))
For systems that process personally identifiable information:
(a) Apply the following processing rules to data elements of personally identifiable information: [Assignment: organization-defined processing rules];
(b) Monitor for permitted processing at the external interfaces to the system and at key internal boundaries within the system;
(c) Document each processing exception; and
(d) Review and remove exceptions that are no longer supported.

Discussion for Boundary Protection | Personally Identifiable Information (SC-7(24))
Managing the processing of personally identifiable information is an important aspect of protecting an individual's privacy. Applying, monitoring for, and documenting exceptions to processing rules ensure that personally identifiable information is processed only in accordance with established privacy requirements.

Boundary Protection | Unclassified National Security System Connections (SC-7(25))

Description for Boundary Protection | Unclassified National Security System Connections (SC-7(25))
Prohibit the direct connection of [Assignment: organization-defined unclassified national security system] to an external network without the use of [Assignment: organization-defined boundary protection device].

Discussion for Boundary Protection | Unclassified National Security System Connections (SC-7(25))
A direct connection is a dedicated physical or virtual connection between two or more systems. Organizations typically do not have complete control over external networks, including the Internet. Boundary protection devices (e.g., firewalls, gateways, and routers) mediate communications and information flows between unclassified national security systems and external networks.

Boundary Protection | Classified National Security System Connections (SC-7(26))

Description for Boundary Protection | Classified National Security System Connections (SC-7(26))
Prohibit the direct connection of a classified national security system to an external network without the use of [Assignment: organization-defined boundary protection device].

Discussion for Boundary Protection | Classified National Security System Connections (SC-7(26))
A direct connection is a dedicated physical or virtual connection between two or more systems. Organizations typically do not have complete control over external networks, including the Internet. Boundary protection devices (e.g., firewalls, gateways, and routers) mediate communications and information flows between classified national security systems and external networks. In addition, approved boundary protection devices (typically managed interface or cross-domain systems) provide information flow enforcement from systems to external networks.

Boundary Protection | Unclassified Non-national Security System Connections (SC-7(27))

Description for Boundary Protection | Unclassified Non-national Security System Connections (SC-7(27))
Prohibit the direct connection of [Assignment: organization-defined unclassified non-national security system] to an external network without the use of [Assignment: organization-defined boundary protection device].

Discussion for Boundary Protection | Unclassified Non-national Security System Connections (SC-7(27))
A direct connection is a dedicated physical or virtual connection between two or more systems. Organizations typically do not have complete control over external networks, including the Internet. Boundary protection devices (e.g., firewalls, gateways, and routers) mediate communications and information flows between unclassified non-national security systems and external networks.

Boundary Protection | Connections to Public Networks (SC-7(28))

Description for Boundary Protection | Connections to Public Networks (SC-7(28))
Prohibit the direct connection of [Assignment: organization-defined system] to a public network.

Discussion for Boundary Protection | Connections to Public Networks (SC-7(28))
A direct connection is a dedicated physical or virtual connection between two or more systems. A public network is a network accessible to the public, including the Internet and organizational extranets with public access.

Boundary Protection | Separate Subnets to Isolate Functions (SC-7(29))

Description for Boundary Protection | Separate Subnets to Isolate Functions (SC-7(29))
Implement [Selection: physically; logically] separate subnetworks to isolate the following critical system components and functions: [Assignment: organization-defined critical system components and functions].

Discussion for Boundary Protection | Separate Subnets to Isolate Functions (SC-7(29))
Separating critical system components and functions from other noncritical system components and functions through separate subnetworks may be necessary to reduce susceptibility to a catastrophic or debilitating breach or compromise that results in system failure. For example, physically separating the command and control function from the in-flight entertainment function through separate subnetworks in a commercial aircraft provides an increased level of assurance in the trustworthiness of critical system functions.

Transmission Confidentiality and Integrity (SC-8)

Description for Transmission Confidentiality and Integrity (SC-8)
Protect the [Selection (one or more): confidentiality; integrity] of transmitted information.

Discussion for Transmission Confidentiality and Integrity (SC-8)
Protecting the confidentiality and integrity of transmitted information applies to internal and external networks as well as 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 or logical means. Physical protection can be achieved by using protected distribution systems. A protected distribution system is a wireline or fiber-optics telecommunications system that includes terminals and adequate electromagnetic, acoustical, electrical, and physical controls to permit its use for the unencrypted transmission of classified information. Logical protection can be achieved by employing encryption techniques.
Organizations that rely on commercial providers who offer transmission services as commodity services rather than as fully dedicated services may find it difficult to obtain the necessary assurances regarding the implementation of needed controls for transmission confidentiality and integrity. In such situations, organizations determine what types of confidentiality or integrity services are available in standard, commercial telecommunications service packages. If it is not feasible to obtain the necessary controls and assurances of control effectiveness through appropriate contracting vehicles, organizations can implement appropriate compensating controls.

Transmission Confidentiality and Integrity | Cryptographic Protection (SC-8(1))

Description for Transmission Confidentiality and Integrity | Cryptographic Protection (SC-8(1))
Implement cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.

Discussion for Transmission Confidentiality and Integrity | Cryptographic Protection (SC-8(1))
Encryption protects information from unauthorized disclosure and modification during transmission. Cryptographic mechanisms that protect the confidentiality and integrity of information during transmission include TLS and IPSec. Cryptographic mechanisms used to protect information integrity include cryptographic hash functions that have applications in digital signatures, checksums, and message authentication codes.

Transmission Confidentiality and Integrity | Pre- and Post-transmission Handling (SC-8(2))

Description for Transmission Confidentiality and Integrity | Pre- and Post-transmission Handling (SC-8(2))
Maintain the [Selection (one or more): confidentiality; integrity] of information during preparation for transmission and during reception.

Discussion for Transmission Confidentiality and Integrity | Pre- and Post-transmission Handling (SC-8(2))
Information can be unintentionally or maliciously disclosed or modified during preparation for transmission or during reception, including during aggregation, at protocol transformation points, and during packing and unpacking. Such unauthorized disclosures or modifications compromise the confidentiality or integrity of the information.

Transmission Confidentiality and Integrity | Cryptographic Protection for Message Externals (SC-8(3))

Description for Transmission Confidentiality and Integrity | Cryptographic Protection for Message Externals (SC-8(3))
Implement cryptographic mechanisms to protect message externals unless otherwise protected by [Assignment: organization-defined alternative physical controls].

Discussion for Transmission Confidentiality and Integrity | Cryptographic Protection for Message Externals (SC-8(3))
Cryptographic protection for message externals addresses protection from the unauthorized disclosure of information. Message externals include message headers and routing 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.

Transmission Confidentiality and Integrity | Conceal or Randomize Communications (SC-8(4))

Description for Transmission Confidentiality and Integrity | Conceal or Randomize Communications (SC-8(4))
Implement cryptographic mechanisms to conceal or randomize communication patterns unless otherwise protected by [Assignment: organization-defined alternative physical controls].

Discussion for Transmission Confidentiality and Integrity | Conceal or Randomize Communications (SC-8(4))
Concealing or randomizing communication patterns addresses protection from unauthorized disclosure of information. Communication patterns include frequency, periods, predictability, and amount. Changes to communications patterns can reveal information with intelligence value, especially when combined with other available information related to the mission and business functions of the organization. Concealing or randomizing communications 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. Encrypting the links 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.

Transmission Confidentiality and Integrity | Protected Distribution System (SC-8(5))

Description for Transmission Confidentiality and Integrity | Protected Distribution System (SC-8(5))
Implement [Assignment: organization-defined protected distribution system] to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.

Discussion for Transmission Confidentiality and Integrity | Protected Distribution System (SC-8(5))
The purpose of a protected distribution system is to deter, detect, and/or make difficult physical access to the communication lines that carry national security information.

Cryptographic Protection | Individuals Without Formal Access Approvals (SC-13(3))

Description for Cryptographic Protection | Individuals Without Formal Access Approvals (SC-13(3))
[Withdrawn: Incorporated into SC-13.]

Discussion for Cryptographic Protection | Individuals Without Formal Access Approvals (SC-13(3))

Network Disconnect (SC-10)

Description for Network Disconnect (SC-10)
Terminate the network connection associated with a communications session at the end of the session or after [Assignment: organization-defined time period] of inactivity.

Discussion for Network Disconnect (SC-10)
Network disconnect applies to internal and external networks. Terminating network connections associated with specific communications sessions includes de-allocating TCP/IP address 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 accesses.

Trusted Path (SC-11)

Description for Trusted Path (SC-11)
a. Provide a [Selection: physically; logically] isolated 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].

Discussion for Trusted Path (SC-11)
Trusted paths are mechanisms by which users can communicate (using input devices such as keyboards) directly with the security functions of systems with the requisite assurance to support security policies. Trusted path mechanisms can only be activated by users or the security functions of organizational systems. User responses that occur via trusted paths are protected from modification by and disclosure to untrusted applications. Organizations employ trusted paths for trustworthy, high-assurance connections between security functions of systems and users, including during system logons. The original implementations of trusted paths employed an out-of-band signal to initiate the path, such as using the <BREAK> key, which does not transmit characters that can be spoofed. In later implementations, a key combination that could not be hijacked was used (e.g., the <CTRL> + <ALT> + <DEL> keys). Such key combinations, however, are platform-specific and may not provide a trusted path implementation in every case. The enforcement of trusted communications paths is provided by a specific implementation that meets the reference monitor concept.

Trusted Path | Irrefutable Communications Path (SC-11(1))

Description for Trusted Path | Irrefutable Communications Path (SC-11(1))
(a) Provide a trusted communications path that is irrefutably distinguishable from other communications paths; and
(b) Initiate the trusted communications path for communications between the [Assignment: organization-defined security functions] of the system and the user.

Discussion for Trusted Path | Irrefutable Communications Path (SC-11(1))
An irrefutable communications path permits the system to initiate a trusted path, which necessitates that the user can unmistakably recognize the source of the communication as a trusted system component. For example, the trusted path may appear in an area of the display that other applications cannot access or be based on the presence of an identifier that cannot be spoofed.

Cryptographic Key Establishment and Management (SC-12)

Description for Cryptographic Key Establishment and Management (SC-12)
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].

Discussion for Cryptographic Key Establishment and Management (SC-12)
Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. Organizations define key management requirements in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and specify appropriate options, parameters, and levels. Organizations manage trust stores to ensure that only approved trust anchors 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.

Cryptographic Key Establishment and Management | Availability (SC-12(1))

Description for Cryptographic Key Establishment and Management | Availability (SC-12(1))
Maintain availability of information in the event of the loss of cryptographic keys by users.

Discussion for Cryptographic Key Establishment and Management | Availability (SC-12(1))
Escrowing of encryption keys is a common practice for ensuring availability in the event of key loss. A forgotten passphrase is an example of losing a cryptographic key.

Cryptographic Key Establishment and Management | Symmetric Keys (SC-12(2))

Description for Cryptographic Key Establishment and Management | Symmetric Keys (SC-12(2))
Produce, control, and distribute symmetric cryptographic keys using [Selection: NIST FIPS-validated; NSA-approved] key management technology and processes.

Discussion for Cryptographic Key Establishment and Management | Symmetric Keys (SC-12(2))
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 800-57-3 provide guidance on cryptographic key management.

Cryptographic Key Establishment and Management | Asymmetric Keys (SC-12(3))

Description for Cryptographic Key Establishment and Management | Asymmetric Keys (SC-12(3))
Produce, control, and distribute asymmetric cryptographic keys using [Selection: NSA-approved key management technology and processes; prepositioned keying material; DoD-approved or DoD-issued Medium Assurance PKI certificates; DoD-approved or DoD-issued Medium Hardware Assurance PKI certificates and hardware security tokens that protect the user's private key; certificates issued in accordance with organization-defined requirements].

Discussion for Cryptographic Key Establishment and Management | Asymmetric Keys (SC-12(3))
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 800-57-3 provide guidance on cryptographic key management.

Cryptographic Protection | Digital Signatures (SC-13(4))

Description for Cryptographic Protection | Digital Signatures (SC-13(4))
[Withdrawn: Incorporated into SC-13.]

Discussion for Cryptographic Protection | Digital Signatures (SC-13(4))

Public Access Protections (SC-14)

Description for Public Access Protections (SC-14)
[Withdrawn: Incorporated into AC-2, AC-3, AC-5, AC-6, SI-3, SI-4, SI-5, SI-7, and SI-10.]

Discussion for Public Access Protections (SC-14)

Cryptographic Key Establishment and Management | Physical Control of Keys (SC-12(6))

Description for Cryptographic Key Establishment and Management | Physical Control of Keys (SC-12(6))
Maintain physical control of cryptographic keys when stored information is encrypted by external service providers.

Discussion for Cryptographic Key Establishment and Management | Physical Control of Keys (SC-12(6))
For organizations that use external service providers (e.g., cloud service 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.

Cryptographic Protection (SC-13)

Description for Cryptographic Protection (SC-13)
a. Determine the [Assignment: organization-defined cryptographic uses]; and
b. Implement the following types of cryptography required for each specified cryptographic use: [Assignment: organization-defined types of cryptography for each specified cryptographic use].

Discussion for Cryptographic Protection (SC-13)
Cryptography can be employed to support a variety of security solutions, including the protection of classified information and controlled unclassified information, the provision and implementation of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances but lack the necessary formal access approvals. Cryptography can also be used to support random number and hash generation. Generally applicable cryptographic standards include FIPS-validated cryptography and NSA-approved cryptography. For example, organizations that need to protect classified information may specify the use of NSA-approved cryptography. Organizations that need to provision and implement digital signatures may specify the use of FIPS-validated cryptography. Cryptography is implemented in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Collaborative Computing Devices and Applications | Blocking Inbound and Outbound Communications Traffic (SC-15(2))

Description for Collaborative Computing Devices and Applications | Blocking Inbound and Outbound Communications Traffic (SC-15(2))
[Withdrawn: Incorporated into SC-7.]

Discussion for Collaborative Computing Devices and Applications | Blocking Inbound and Outbound Communications Traffic (SC-15(2))

Voice Over Internet Protocol (SC-19)

Description for Voice Over Internet Protocol (SC-19)
[Withdrawn: Technology-specific; addressed as any other technology or protocol.]

Discussion for Voice Over Internet Protocol (SC-19)

Secure Name/address Resolution Service (authoritative Source) | Child Subspaces (SC-20(1)) Description for Secure Name/address Resolution Service (authoritative Source) | Child Subspaces (SC-20(1)) [Withdrawn: Incorporated into SC-20.] Discussion for Secure Name/address Resolution Service (authoritative Source) | Child Subspaces (SC-20(1))
Secure Name/address Resolution Service (recursive or Caching Resolver) | Data Origin and Integrity (SC-21(1)) Description for Secure Name/address Resolution Service (recursive or Caching Resolver) | Data Origin and Integrity (SC-21(1)) [Withdrawn: Incorporated into SC-21.] Discussion for Secure Name/address Resolution Service (recursive or Caching Resolver) | Data Origin and Integrity (SC-21(1))
Session Authenticity | User-initiated Logouts and Message Displays (SC-23(2)) Description for Session Authenticity | User-initiated Logouts and Message Displays (SC-23(2)) [Withdrawn: Incorporated into AC-12(1).] Discussion for Session Authenticity | User-initiated Logouts and Message Displays (SC-23(2))

Collaborative Computing Devices and Applications (SC-15)

Description for Collaborative Computing Devices and Applications (SC-15)
a. Prohibit remote activation of collaborative computing devices and applications with the following exceptions: [Assignment: organization-defined exceptions where remote activation is to be allowed]; and
b. Provide an explicit indication of use to users physically present at the devices.

Discussion for Collaborative Computing Devices and Applications (SC-15)
Collaborative computing devices and applications include remote meeting devices and applications, networked white boards, cameras, and microphones. The explicit indication of use includes signals to users when collaborative computing devices and applications are activated.

Collaborative Computing Devices and Applications | Physical or Logical Disconnect (SC-15(1))

Description for Collaborative Computing Devices and Applications | Physical or Logical Disconnect (SC-15(1))
Provide [Selection (one or more): physical; logical] disconnect of collaborative computing devices in a manner that supports ease of use.

Discussion for Collaborative Computing Devices and Applications | Physical or Logical Disconnect (SC-15(1))
Failing to disconnect from collaborative computing devices can result in subsequent compromises of organizational information. Providing easy methods to disconnect from such devices after a collaborative computing session ensures that participants carry out the disconnect activity without having to go through complex and tedious procedures. Disconnect from collaborative computing devices can be manual or automatic.

Session Authenticity | Unique Session Identifiers with Randomization (SC-23(4))

Description for Session Authenticity | Unique Session Identifiers with Randomization (SC-23(4))
[Withdrawn: Incorporated into SC-23(3).]

Discussion for Session Authenticity | Unique Session Identifiers with Randomization (SC-23(4))

Collaborative Computing Devices and Applications | Disabling and Removal in Secure Work Areas (SC-15(3))

Description for Collaborative Computing Devices and Applications | Disabling and Removal in Secure Work Areas (SC-15(3))
Disable or remove collaborative computing devices and applications from [Assignment: organization-defined systems or system components] in [Assignment: organization-defined secure work areas].

Discussion for Collaborative Computing Devices and Applications | Disabling and Removal in Secure Work Areas (SC-15(3))
Failing to disable or remove collaborative computing devices and applications from systems or system components can result in compromises of information, including eavesdropping on conversations. A Sensitive Compartmented Information Facility (SCIF) is an example of a secure work area.

Collaborative Computing Devices and Applications | Explicitly Indicate Current Participants (SC-15(4))

Description for Collaborative Computing Devices and Applications | Explicitly Indicate Current Participants (SC-15(4))
Provide an explicit indication of current participants in [Assignment: organization-defined online meetings and teleconferences].

Discussion for Collaborative Computing Devices and Applications | Explicitly Indicate Current Participants (SC-15(4))
Explicitly indicating current participants prevents unauthorized individuals from participating in collaborative computing sessions without the explicit knowledge of other participants.

Transmission of Security and Privacy Attributes (SC-16)

Description for Transmission of Security and Privacy Attributes (SC-16)
Associate [Assignment: organization-defined security and privacy attributes] with information exchanged between systems and between system components.

Discussion for Transmission of Security and Privacy Attributes (SC-16)
Security and privacy attributes can be explicitly or implicitly associated with the information contained in organizational systems or system components. Attributes are abstractions that represent the basic properties or characteristics of an entity with respect to protecting information or the management of personally identifiable information. Attributes are typically associated with internal data structures, including records, buffers, and files within the system. Security and privacy attributes are used to implement access control and information flow control policies; reflect special dissemination, management, or distribution instructions, including permitted uses of personally identifiable information; or support other aspects of the information security and privacy policies. Privacy attributes may be used independently or in conjunction with security attributes.

Transmission of Security and Privacy Attributes | Integrity Verification (SC-16(1))

Description for Transmission of Security and Privacy Attributes | Integrity Verification (SC-16(1))
Verify the integrity of transmitted security and privacy attributes.

Discussion for Transmission of Security and Privacy Attributes | Integrity Verification (SC-16(1))
Part of verifying the integrity of transmitted information is ensuring that security and privacy attributes that are associated with such information have not been modified in an unauthorized manner. Unauthorized modification of security or privacy attributes can result in a loss of integrity for transmitted information.

Transmission of Security and Privacy Attributes | Anti-spoofing Mechanisms (SC-16(2))

Description for Transmission of Security and Privacy Attributes | Anti-spoofing Mechanisms (SC-16(2))
Implement anti-spoofing mechanisms to prevent adversaries from falsifying the security attributes indicating the successful application of the security process.

Discussion for Transmission of Security and Privacy Attributes | Anti-spoofing Mechanisms (SC-16(2))
Some attack vectors operate by altering the security attributes of an information system to intentionally and maliciously implement an insufficient level of security within the system. The alteration of attributes leads organizations to believe that a greater number of security functions are in place and operational than have actually been implemented.

Transmission of Security and Privacy Attributes | Cryptographic Binding (SC-16(3))

Description for Transmission of Security and Privacy Attributes | Cryptographic Binding (SC-16(3))
Implement [Assignment: organization-defined mechanisms or techniques] to bind security and privacy attributes to transmitted information.

Discussion for Transmission of Security and Privacy Attributes | Cryptographic Binding (SC-16(3))
Cryptographic mechanisms and techniques can provide strong security and privacy attribute binding to transmitted information to help ensure the integrity of such information.

Public Key Infrastructure Certificates (SC-17)

Description for Public Key Infrastructure Certificates (SC-17)
a. Issue public key certificates under an [Assignment: organization-defined certificate policy] or obtain public key certificates from an approved service provider; and
b. Include only approved trust anchors in trust stores or certificate stores managed by the organization.

Discussion for Public Key Infrastructure Certificates (SC-17)
Public key infrastructure (PKI) certificates are certificates with visibility external to organizational systems and certificates related to the internal operations of systems, such as application-specific time services. In cryptographic systems with a hierarchical structure, a trust anchor is an authoritative source (i.e., a certificate authority) for which trust is assumed and not derived. A root certificate for a PKI system is an example of a trust anchor. A trust store or certificate store maintains a list of trusted root certificates.

Mobile Code (SC-18)

Description for Mobile Code (SC-18)
a. Define acceptable and unacceptable mobile code and mobile code technologies; and
b. Authorize, monitor, and control the use of mobile code within the system.

Discussion for Mobile Code (SC-18)
Mobile code includes any program, application, or content that can be transmitted across a network (e.g., embedded in an email, document, or website) and executed on a remote system. Decisions regarding the use of mobile code within organizational systems are based on the potential for the code to cause damage to the systems if used maliciously. Mobile code technologies include Java applets, JavaScript, HTML5, WebGL, and VBScript. Usage restrictions and implementation guidelines apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations and devices, including notebook computers and smart phones. Mobile code policy and procedures address specific actions taken to prevent the development, acquisition, and introduction of unacceptable mobile code within organizational systems, including requiring mobile code to be digitally signed by a trusted source.

Mobile Code | Identify Unacceptable Code and Take Corrective Actions (SC-18(1))

Description for Mobile Code | Identify Unacceptable Code and Take Corrective Actions (SC-18(1))
Identify [Assignment: organization-defined unacceptable mobile code] and take [Assignment: organization-defined corrective actions].

Discussion for Mobile Code | Identify Unacceptable Code and Take Corrective Actions (SC-18(1))
Corrective actions when unacceptable mobile code is detected include blocking, quarantine, or alerting administrators. Blocking includes preventing the transmission of word processing files with embedded macros when such macros have been determined to be unacceptable mobile code.

Mobile Code | Acquisition, Development, and Use (SC-18(2))

Description for Mobile Code | Acquisition, Development, and Use (SC-18(2))
Verify that the acquisition, development, and use of mobile code to be deployed in the system meets [Assignment: organization-defined mobile code requirements].

Discussion for Mobile Code | Acquisition, Development, and Use (SC-18(2))
None.

Mobile Code | Prevent Downloading and Execution (SC-18(3))

Description for Mobile Code | Prevent Downloading and Execution (SC-18(3))
Prevent the download and execution of [Assignment: organization-defined unacceptable mobile code].

Discussion for Mobile Code | Prevent Downloading and Execution (SC-18(3))
None.

Mobile Code | Prevent Automatic Execution (SC-18(4))

Description for Mobile Code | Prevent Automatic Execution (SC-18(4))
Prevent the automatic execution of mobile code in [Assignment: organization-defined software applications] and enforce [Assignment: organization-defined actions] prior to executing the code.

Discussion for Mobile Code | Prevent Automatic Execution (SC-18(4))
Actions enforced before executing mobile code include prompting users prior to opening email attachments or clicking on web links. Preventing the automatic execution of mobile code includes disabling auto-execute features on system components that employ portable storage devices, such as compact discs, digital versatile discs, and universal serial bus devices.

Mobile Code | Allow Execution Only in Confined Environments (SC-18(5))

Description for Mobile Code | Allow Execution Only in Confined Environments (SC-18(5))
Allow execution of permitted mobile code only in confined virtual machine environments.

Discussion for Mobile Code | Allow Execution Only in Confined Environments (SC-18(5))
Permitting the execution of mobile code only in confined virtual machine environments helps prevent the introduction of malicious code into other systems and system components.

Decoys | Detection of Malicious Code (SC-26(1))

Description for Decoys | Detection of Malicious Code (SC-26(1))
[Withdrawn: Incorporated into SC-35.]

Discussion for Decoys | Detection of Malicious Code (SC-26(1))

Secure Name/address Resolution Service (authoritative Source) (SC-20)

Description for Secure Name/address Resolution Service (authoritative Source) (SC-20)
a. Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and
b. Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

Discussion for Secure Name/address Resolution Service (authoritative Source) (SC-20)
Providing authoritative source information enables external clients, including remote Internet clients, to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service. Systems that provide name and address resolution services include domain name system (DNS) servers. Additional artifacts include DNS Security Extensions (DNSSEC) digital signatures and cryptographic keys. Authoritative data includes DNS resource records. The means for indicating the security status of child zones include the use of delegation signer resource records in the DNS. Systems that use technologies other than the DNS to map between host and service names and network addresses provide other means to assure the authenticity and integrity of response data.

Concealment and Misdirection | Virtualization Techniques (SC-30(1))

Description for Concealment and Misdirection | Virtualization Techniques (SC-30(1))
[Withdrawn: Incorporated into SC-29(1).]

Discussion for Concealment and Misdirection | Virtualization Techniques (SC-30(1))

Secure Name/address Resolution Service (authoritative Source) | Data Origin and Integrity (SC-20(2))

Description for Secure Name/address Resolution Service (authoritative Source) | Data Origin and Integrity (SC-20(2))
Provide data origin and integrity protection artifacts for internal name/address resolution queries.

Discussion for Secure Name/address Resolution Service (authoritative Source) | Data Origin and Integrity (SC-20(2))
None.

Secure Name/address Resolution Service (recursive or Caching Resolver) (SC-21)

Description for Secure Name/address Resolution Service (recursive or Caching Resolver) (SC-21)
Request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

Discussion for Secure Name/address Resolution Service (recursive or Caching Resolver) (SC-21)
Each client of name resolution services either performs this validation on its own or has authenticated channels to trusted validation providers. Systems that provide name and address resolution services for local clients include recursive resolving or caching domain name system (DNS) servers. DNS client resolvers either perform validation of DNSSEC signatures, or clients use authenticated channels to recursive resolvers that perform such validations. Systems that use technologies other than the DNS to map between host and service names and network addresses provide some other means to enable clients to verify the authenticity and integrity of response data.

Transmission Preparation Integrity (SC-33)

Description for Transmission Preparation Integrity (SC-33)
[Withdrawn: Incorporated into SC-8.]

Discussion for Transmission Preparation Integrity (SC-33)

Architecture and Provisioning for Name/address Resolution Service (SC-22)

Description for Architecture and Provisioning for Name/address Resolution Service (SC-22)
Ensure the systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal and external role separation.

Discussion for Architecture and Provisioning for Name/address Resolution Service (SC-22)
Systems that provide name and address resolution services include domain name system (DNS) servers. To eliminate single points of failure in systems and enhance redundancy, organizations employ at least two authoritative domain name system servers—one configured as the primary server and the other configured as the secondary server. Additionally, organizations typically deploy the servers in two geographically separated network subnetworks (i.e., not located in the same physical facility). For role separation, DNS servers with internal roles only process name and address resolution requests from within organizations (i.e., from internal clients). DNS servers with external roles only process name and address resolution information requests from clients external to organizations (i.e., on external networks, including the Internet). Organizations specify clients that can access authoritative DNS servers in certain roles (e.g., by address ranges and explicit lists).

Session Authenticity (SC-23)

Description for Session Authenticity (SC-23)
Protect the authenticity of communications sessions.

Discussion for Session Authenticity (SC-23)
Protecting session authenticity addresses communications protection at the session level, not at the packet level. Such protection establishes grounds for confidence at both ends of communications sessions in the ongoing identities of other parties and the validity of transmitted information. Authenticity protection includes protecting against man-in-the-middle attacks, session hijacking, and the insertion of false information into sessions.

Session Authenticity | Invalidate Session Identifiers at Logout (SC-23(1))

Description for Session Authenticity | Invalidate Session Identifiers at Logout (SC-23(1))
Invalidate session identifiers upon user logout or other session termination.

Discussion for Session Authenticity | Invalidate Session Identifiers at Logout (SC-23(1))
Invalidating session identifiers at logout curtails the ability of adversaries to capture and continue to employ previously valid session IDs.

Non-modifiable Executable Programs | Hardware-based Protection (SC-34(3))

Description for Non-modifiable Executable Programs | Hardware-based Protection (SC-34(3))
[Withdrawn: Moved to SC-51.]

Discussion for Non-modifiable Executable Programs | Hardware-based Protection (SC-34(3))

Session Authenticity | Unique System-generated Session Identifiers (SC-23(3))

Description for Session Authenticity | Unique System-generated Session Identifiers (SC-23(3))
Generate a unique session identifier for each session with [Assignment: organization-defined randomness requirements] and recognize only session identifiers that are system-generated.

Discussion for Session Authenticity | Unique System-generated Session Identifiers (SC-23(3))
Generating unique session identifiers curtails the ability of adversaries to reuse previously valid session IDs. Employing the concept of randomness in the generation of unique session identifiers protects against brute-force attacks to determine future session identifiers.

Information in Shared System Resources | Security Levels (SC-4(1))

Description for Information in Shared System Resources | Security Levels (SC-4(1))
[Withdrawn: Incorporated into SC-4.]

Discussion for Information in Shared System Resources | Security Levels (SC-4(1))

Session Authenticity | Allowed Certificate Authorities (SC-23(5))

Description for Session Authenticity | Allowed Certificate Authorities (SC-23(5))
Only allow the use of [Assignment: organization-defined certificate authorities] for verification of the establishment of protected sessions.

Discussion for Session Authenticity | Allowed Certificate Authorities (SC-23(5))
Reliance on certificate authorities for the establishment of secure sessions includes the use of Transport Layer Security (TLS) certificates. These certificates, after verification by their respective certificate authorities, facilitate the establishment of protected sessions between web clients and web servers.

Fail in Known State (SC-24)

Description for Fail in Known State (SC-24)
Fail to a [Assignment: organization-defined known system state] for the following failures on the indicated components while preserving [Assignment: organization-defined system state information] in failure: [Assignment: list of organization-defined types of system failures on organization-defined system components].

Discussion for Fail in Known State (SC-24)
Failure in a known state addresses security concerns in accordance with the mission and business needs of organizations. Failure in a known state prevents the loss of confidentiality, integrity, or availability of information in the event of failures of organizational systems or system components. Failure in a known safe state helps to prevent systems from failing to a state that may cause injury to individuals or destruction to property. Preserving system state information facilitates system restart and return to the operational mode with less disruption of mission and business processes.

Thin Nodes (SC-25)

Description for Thin Nodes (SC-25)
Employ minimal functionality and information storage on the following system components: [Assignment: organization-defined system components].

Discussion for Thin Nodes (SC-25)
The deployment of system components with minimal functionality reduces the need to secure every endpoint and may reduce the exposure of information, systems, and services to attacks. Reduced or minimal functionality includes diskless nodes and thin client technologies.

Decoys (SC-26)

Description for Decoys (SC-26)
Include components within organizational systems specifically designed to be the target of malicious attacks for detecting, deflecting, and analyzing such attacks.

Discussion for Decoys (SC-26)
Decoys (i.e., honeypots, honeynets, or deception nets) are established to attract adversaries and deflect attacks away from the operational systems that support organizational mission and business functions. Use of decoys requires some supporting isolation measures to ensure that any deflected malicious code does not infect organizational systems. Depending on the specific usage of the decoy, consultation with the Office of the General Counsel before deployment may be needed.

Sensor Capability and Data | Prohibit Use of Devices (SC-42(3))

Description for Sensor Capability and Data | Prohibit Use of Devices (SC-42(3))
[Withdrawn: Incorporated into SC-42.]

Discussion for Sensor Capability and Data | Prohibit Use of Devices (SC-42(3))

Platform-independent Applications (SC-27)

Description for Platform-independent Applications (SC-27)
Include within organizational systems the following platform independent applications: [Assignment: organization-defined platform-independent applications].

Discussion for Platform-independent Applications (SC-27)
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 reconstitution on different platforms. Application portability and the ability to reconstitute on different platforms increase the availability of mission-essential functions within organizations in situations where systems with specific operating systems are under attack.

Protection of Information at Rest (SC-28)

Description for Protection of Information at Rest (SC-28)
Protect the [Selection (one or more): confidentiality; integrity] of the following information at rest: [Assignment: organization-defined information at rest].

Discussion for Protection of Information at Rest (SC-28)
Information at rest refers to the state of information when it is not in process or in transit and is located on system components. Such components include internal or external hard disk drives, storage area network devices, or databases. However, the focus of protecting information at rest is not on the type of storage device or frequency of access but rather on the state of the information. Information at rest addresses the confidentiality and integrity of information and covers user information and system information. System-related information that requires protection includes configurations or rule sets for firewalls, intrusion detection and prevention systems, filtering routers, and authentication information.
Organizations may employ different mechanisms to achieve confidentiality and integrity protections, including the use of cryptographic mechanisms and file share scanning. Integrity protection can be achieved, for example, by implementing write-once-read-many (WORM) technologies. When adequate protection of information at rest cannot otherwise be achieved, organizations may employ other controls, including frequent scanning to identify malicious code at rest and secure offline storage in lieu of online storage.

Protection of Information at Rest | Cryptographic Protection (SC-28(1))

Description for Protection of Information at Rest | Cryptographic Protection (SC-28(1))
Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information].

Discussion for Protection of Information at Rest | Cryptographic Protection (SC-28(1))
The selection of cryptographic mechanisms is based on the need to protect the confidentiality and integrity of organizational information. The strength of mechanism is commensurate with the security category or classification of the information. Organizations have the flexibility to encrypt information on system components or media or encrypt data structures, including files, records, or fields.

Protection of Information at Rest | Offline Storage (SC-28(2))

Description for Protection of Information at Rest | Offline Storage (SC-28(2))
Remove the following information from online storage and store offline in a secure location: [Assignment: organization-defined information].

Discussion for Protection of Information at Rest | Offline Storage (SC-28(2))
Removing organizational information from online storage to offline storage eliminates the possibility of individuals gaining unauthorized access to the information through a network. Therefore, organizations may choose to move information to offline storage in lieu of protecting such information in online storage.

Protection of Information at Rest | Cryptographic Keys (SC-28(3))

Description for Protection of Information at Rest | Cryptographic Keys (SC-28(3))
Provide protected storage for cryptographic keys [Selection: [Assignment: organization-defined safeguards]; hardware-protected key store].

Discussion for Protection of Information at Rest | Cryptographic Keys (SC-28(3))
A Trusted Platform Module (TPM) is an example of a hardware-protected data store that can be used to protect cryptographic keys.

Heterogeneity (SC-29)

Description for Heterogeneity (SC-29)
Employ a diverse set of information technologies for the following system components in the implementation of the system: [Assignment: organization-defined system components].

Discussion for Heterogeneity (SC-29)
Increasing the diversity of information technologies within organizational systems reduces the impact of potential exploitations or compromises of specific technologies. Such diversity protects against common mode failures, including those failures induced by supply chain attacks. Diversity in information technologies also reduces the likelihood that the means adversaries use to compromise one system component will be effective against other system components, thus further increasing the adversary work factor to successfully complete planned attacks. An increase in diversity may add complexity and management overhead that could ultimately lead to mistakes and unauthorized configurations.

Heterogeneity | Virtualization Techniques (SC-29(1))

Description for Heterogeneity | Virtualization Techniques (SC-29(1))
Employ virtualization techniques to support the deployment of a diversity of operating systems and applications that are changed [Assignment: organization-defined frequency].

Discussion for Heterogeneity | Virtualization Techniques (SC-29(1))
While frequent changes to operating systems and applications can pose significant configuration management challenges, the changes can result in an increased work factor for adversaries to conduct successful attacks. Changing virtual operating systems or applications, as opposed to changing actual operating systems or applications, provides virtual changes that impede attacker success while reducing configuration management efforts. Virtualization techniques can assist in isolating untrustworthy software or software of dubious provenance into confined execution environments.

Concealment and Misdirection (SC-30)

Description for Concealment and Misdirection (SC-30)
Employ the following concealment and misdirection techniques for [Assignment: organization-defined systems] at [Assignment: organization-defined time periods] to confuse and mislead adversaries: [Assignment: organization-defined concealment and misdirection techniques].

Discussion for Concealment and Misdirection (SC-30)
Concealment and misdirection techniques can significantly reduce the targeting capabilities of adversaries (i.e., window of opportunity and available attack surface) to initiate and complete attacks. For example, virtualization techniques provide organizations with the ability to disguise systems, potentially reducing the likelihood of successful attacks without the cost of having multiple platforms. The increased use of concealment and misdirection techniques and methods—including randomness, uncertainty, and virtualization—may sufficiently confuse and mislead adversaries and subsequently increase the risk of discovery and/or exposing tradecraft. Concealment and misdirection techniques may provide additional time to perform core mission and business functions. The implementation of concealment and misdirection techniques may add to the complexity and management overhead required for the system.

Boundary Protection | Physically Separated Subnetworks (SC-7(1))

Description for Boundary Protection | Physically Separated Subnetworks (SC-7(1))
[Withdrawn: Incorporated into SC-7.]

Discussion for Boundary Protection | Physically Separated Subnetworks (SC-7(1))

Concealment and Misdirection | Randomness (SC-30(2))

Description for Concealment and Misdirection | Randomness (SC-30(2))
Employ [Assignment: organization-defined techniques] to introduce randomness into organizational operations and assets.

Discussion for Concealment and Misdirection | Randomness (SC-30(2))
Randomness introduces increased levels of uncertainty for adversaries regarding the actions that organizations take to defend their systems against attacks. Such actions may impede the ability of adversaries to correctly target information resources of organizations that support critical missions or business functions. Uncertainty may also cause adversaries to hesitate before initiating or continuing attacks. Misdirection techniques that involve randomness include performing certain routine actions at different times of day, employing different information technologies, using different suppliers, and rotating roles and responsibilities of organizational personnel.

Concealment and Misdirection | Change Processing and Storage Locations (SC-30(3))

Description for Concealment and Misdirection | Change Processing and Storage Locations (SC-30(3))
Change the location of [Assignment: organization-defined processing and/or storage] [Selection: [Assignment: organization-defined time frequency]; at random time intervals]].

Discussion for Concealment and Misdirection | Change Processing and Storage Locations (SC-30(3))
Adversaries target critical mission and business functions and the systems that support those mission and business functions while also trying to minimize the exposure of their existence and tradecraft. The static, homogeneous, and deterministic nature of organizational systems targeted by adversaries make such systems more susceptible to attacks with less adversary cost and effort to be successful. Changing processing and storage locations (also referred to as moving target defense) addresses the advanced persistent threat using techniques such as virtualization, distributed processing, and replication. This enables organizations to relocate the system components (i.e., processing, storage) that support critical mission and business functions. Changing the locations of processing activities and/or storage sites introduces a degree of uncertainty into the targeting activities of adversaries. The targeting uncertainty increases the work factor of adversaries and makes compromises or breaches of the organizational systems more difficult and time-consuming. It also increases the chances that adversaries may inadvertently disclose certain aspects of their tradecraft while attempting to locate critical organizational resources.

Concealment and Misdirection | Misleading Information (SC-30(4))

Description for Concealment and Misdirection | Misleading Information (SC-30(4))
Employ realistic, but misleading information in [Assignment: organization-defined system components] about its security state or posture.

Discussion for Concealment and Misdirection | Misleading Information (SC-30(4))
Employing misleading information is intended to confuse potential adversaries regarding the nature and extent of controls deployed by organizations. Thus, adversaries may employ incorrect and ineffective attack techniques. One technique for misleading adversaries is for organizations to place misleading information regarding the specific controls deployed in external systems that are known to be targeted by adversaries. Another technique is the use of deception nets that mimic actual aspects of organizational systems but use, for example, out-of-date software configurations.

Concealment and Misdirection | Concealment of System Components (SC-30(5))

Description for Concealment and Misdirection | Concealment of System Components (SC-30(5))
Employ the following techniques to hide or conceal [Assignment: organization-defined system components]: [Assignment: organization-defined techniques].

Discussion for Concealment and Misdirection | Concealment of System Components (SC-30(5))
By hiding, disguising, or concealing critical system components, organizations may be able to decrease the probability that adversaries target and successfully compromise those assets. Potential means to hide, disguise, or conceal system components include the configuration of routers or the use of encryption or virtualization techniques.

Covert Channel Analysis (SC-31)

Description for Covert Channel Analysis (SC-31)
a. Perform a covert channel analysis to identify those aspects of communications within the system that are potential avenues for covert [Selection (one or more): storage; timing] channels; and
b. Estimate the maximum bandwidth of those channels.

Discussion for Covert Channel Analysis (SC-31)
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 unauthorized information flows across security domains, such as in the case of systems that contain export-controlled information and have connections to external networks (i.e., 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.

Covert Channel Analysis | Test Covert Channels for Exploitability (SC-31(1))

Description for Covert Channel Analysis | Test Covert Channels for Exploitability (SC-31(1))
Test a subset of the identified covert channels to determine the channels that are exploitable.

Discussion for Covert Channel Analysis | Test Covert Channels for Exploitability (SC-31(1))
None.

Covert Channel Analysis | Maximum Bandwidth (SC-31(2))

Description for Covert Channel Analysis | Maximum Bandwidth (SC-31(2))
Reduce the maximum bandwidth for identified covert [Selection (one or more): storage; timing] channels to [Assignment: organization-defined values].

Discussion for Covert Channel Analysis | Maximum Bandwidth (SC-31(2))
The complete elimination of covert channels, especially covert timing channels, is usually not possible without significant performance impacts.

Covert Channel Analysis | Measure Bandwidth in Operational Environments (SC-31(3))

Description for Covert Channel Analysis | Measure Bandwidth in Operational Environments (SC-31(3))
Measure the bandwidth of [Assignment: organization-defined subset of identified covert channels] in the operational environment of the system.

Discussion for Covert Channel Analysis | Measure Bandwidth in Operational Environments (SC-31(3))
Measuring covert channel bandwidth in specified operational environments helps organizations determine how much information can be covertly leaked before such leakage adversely affects mission or business functions. Covert channel bandwidth may be significantly different when measured in settings that are independent of

the specific environments of operation, including laboratories or system development environments.

System Partitioning (SC-32)

Description for System Partitioning (SC-32)
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].

Discussion for System Partitioning (SC-32)
System partitioning is part of a defense-in-depth protection strategy. Organizations determine the degree of physical separation of system components. Physical separation options include physically distinct components in separate racks in the same room, critical components in separate rooms, and geographical separation of critical components. Security categorization can guide the selection of candidates for domain partitioning. Managed interfaces restrict or prohibit network access and information flow among partitioned system components.

System Partitioning | Separate Physical Domains for Privileged Functions (SC-32(1))

Description for System Partitioning | Separate Physical Domains for Privileged Functions (SC-32(1))
Partition privileged functions into separate physical domains.

Discussion for System Partitioning | Separate Physical Domains for Privileged Functions (SC-32(1))
Privileged functions that operate in a single physical domain may represent a single point of failure if that domain becomes compromised or experiences a denial of service.

Boundary Protection | Public Access (SC-7(2))

Description for Boundary Protection | Public Access (SC-7(2))
[Withdrawn: Incorporated into SC-7.]

Discussion for Boundary Protection | Public Access (SC-7(2))

Non-modifiable Executable Programs (SC-34)

Description for Non-modifiable Executable Programs (SC-34)
For [Assignment: organization-defined system components], load and execute:
a. The operating environment from hardware-enforced, read-only media; and
b. The following applications from hardware-enforced, read-only media: [Assignment: organization-defined applications].

Discussion for Non-modifiable Executable Programs (SC-34)
The operating environment for a system contains the code that hosts applications, including operating systems, executives, or virtual machine monitors (i.e., hypervisors). It can also include certain applications that run directly on hardware platforms. Hardware-enforced, read-only media include Compact Disc-Recordable (CD-R) and Digital Versatile Disc-Recordable (DVD-R) disk drives as well as one-time, programmable, read-only memory. The use of non-modifiable storage ensures the integrity of software from the point of creation of the read-only

image. The use of reprogrammable, read-only memory can be accepted as read-only media provided that integrity can be adequately protected from the point of initial writing to the insertion of the memory into the system, and there are reliable hardware protections against reprogramming the memory while installed in organizational systems.

Non-modifiable Executable Programs | No Writable Storage (SC-34(1))

Description for Non-modifiable Executable Programs | No Writable Storage (SC-34(1))
Employ [Assignment: organization-defined system components] with no writeable storage that is persistent across component restart or power on/off.

Discussion for Non-modifiable Executable Programs | No Writable Storage (SC-34(1))
Disallowing writeable storage eliminates the possibility of malicious code insertion via persistent, writeable storage within the designated system components. The restriction applies to fixed and removable storage, with the latter being addressed either directly or as specific restrictions imposed through access controls for mobile devices.

Non-modifiable Executable Programs | Integrity Protection on Read-only Media (SC-34(2))

Description for Non-modifiable Executable Programs | Integrity Protection on Read-only Media (SC-34(2))
Protect the integrity of information prior to storage on read-only media and control the media after such information has been recorded onto the media.

Discussion for Non-modifiable Executable Programs | Integrity Protection on Read-only Media (SC-34(2))
Controls prevent the substitution of media into systems or the reprogramming of programmable read-only media prior to installation into the systems. Integrity protection controls include a combination of prevention, detection, and response.

Boundary Protection | Response to Recognized Failures (SC-7(6))

Description for Boundary Protection | Response to Recognized Failures (SC-7(6))
[Withdrawn: Incorporated into SC-7(18).]

Discussion for Boundary Protection | Response to Recognized Failures (SC-7(6))

External Malicious Code Identification (SC-35)

Description for External Malicious Code Identification (SC-35)
Include system components that proactively seek to identify network-based malicious code or malicious websites.

Discussion for External Malicious Code Identification (SC-35)
External malicious code identification differs from decoys 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 infect organizational systems. Virtualization is a common technique for achieving such isolation.

Distributed Processing and Storage (SC-36)

Description for Distributed Processing and Storage (SC-36)
Distribute the following processing and storage components across multiple [Selection: physical locations; logical domains]: [Assignment: organization-defined processing and storage components].

Discussion for Distributed Processing and Storage (SC-36)
Distributing processing and storage across multiple physical locations or logical domains provides a degree of redundancy or overlap for organizations. The redundancy and overlap increase the work factor of adversaries to adversely impact organizational operations, assets, and individuals. The use of distributed processing and storage does not assume a single primary processing or storage location. Therefore, it allows for parallel processing and storage.

Distributed Processing and Storage | Polling Techniques (SC-36(1))

Description for Distributed Processing and Storage | Polling Techniques (SC-36(1))
(a) Employ polling 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].

Discussion for Distributed Processing and Storage | Polling Techniques (SC-36(1))
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, the distribution of processing and 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.

Distributed Processing and Storage | Synchronization (SC-36(2))

Description for Distributed Processing and Storage | Synchronization (SC-36(2))
Synchronize the following duplicate systems or system components: [Assignment: organization-defined duplicate systems or system components].

Discussion for Distributed Processing and Storage | Synchronization (SC-36(2))
SC-36 and CP-9(6) require the duplication of systems or system components in distributed locations. The 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.

Out-of-band Channels (SC-37)

Description for Out-of-band Channels (SC-37)
Employ the following out-of-band channels for the physical delivery or electronic transmission of [Assignment: organization-defined information, system components, or devices] to [Assignment: organization-defined individuals or systems]: [Assignment: organization-defined out-of-band channels].

Discussion for Out-of-band Channels (SC-37)
Out-of-band channels include local, non-network accesses to systems; network paths physically separate from network paths used for operational traffic; or non-electronic paths, such as the U.S. Postal Service. The use of out-of-band channels is contrasted with the use of in-band channels (i.e., the same channels) 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 transmission of organizational items, including authenticators and credentials; 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.

Out-of-band Channels | Ensure Delivery and Transmission (SC-37(1))

Description for Out-of-band Channels | Ensure Delivery and Transmission (SC-37(1))
Employ [Assignment: organization-defined controls] to ensure that only [Assignment: organization-defined individuals or systems] receive the following information, system components, or devices: [Assignment: organization-defined information, system components, or devices].

Discussion for Out-of-band Channels | Ensure Delivery and Transmission (SC-37(1))
Techniques employed by organizations to ensure that only designated systems or individuals receive certain information, system components, or devices include sending authenticators via an approved courier service but requiring recipients to show some form of government-issued photographic identification as a condition of receipt.

Operations Security (SC-38)

Description for Operations Security (SC-38)
Employ the following operations security controls to protect key organizational information throughout the system development life cycle: [Assignment: organization-defined operations security controls].

Discussion for Operations Security (SC-38)
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, potential suppliers, and other non-

organizational elements and individuals. Information critical to organizational mission 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.

Process Isolation (SC-39)

Description for Process Isolation (SC-39)
Maintain a separate execution domain for each executing system process.

Discussion for Process Isolation (SC-39)
Systems can maintain separate execution domains for each executing process by assigning each process a separate address space. Each system process has a distinct address space so that communication between processes is performed in a manner controlled through the security functions, and one process cannot modify the executing code of another process. Maintaining separate execution domains for executing processes can be achieved, for example, by implementing separate address spaces. 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 untrusted software to other system resources. The capability to maintain separate execution domains is available in commercial operating systems that employ multi-state processor technologies.

Process Isolation | Hardware Separation (SC-39(1))

Description for Process Isolation | Hardware Separation (SC-39(1))
Implement hardware separation mechanisms to facilitate process isolation.

Discussion for Process Isolation | Hardware Separation (SC-39(1))
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.

Process Isolation | Separate Execution Domain Per Thread (SC-39(2))

Description for Process Isolation | Separate Execution Domain Per Thread (SC-39(2))
Maintain a separate execution domain for each thread in [Assignment: organization-defined multi-threaded processing].

Discussion for Process Isolation | Separate Execution Domain Per Thread (SC-39(2))
None.

Wireless Link Protection (SC-40)

Description for Wireless Link Protection (SC-40)
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].

Discussion for Wireless Link Protection (SC-40)
Wireless link protection applies to internal and external wireless communication links that may be 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 not be possible to implement wireless link protections to the extent necessary to meet organizational security requirements.

Wireless Link Protection | Electromagnetic Interference (SC-40(1))

Description for Wireless Link Protection | Electromagnetic Interference (SC-40(1))
Implement cryptographic mechanisms that achieve [Assignment: organization-defined level of protection] against the effects of intentional electromagnetic interference.

Discussion for Wireless Link Protection | Electromagnetic Interference (SC-40(1))
The implementation of cryptographic mechanisms for electromagnetic interference protects systems 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 coincidentally mitigate the effects of unintentional jamming due to interference from legitimate transmitters that share the same spectrum. Mission requirements, projected threats, concept of operations, and laws, executive orders, directives, regulations, policies, and standards determine levels of wireless link availability, cryptography needed, and performance.

Wireless Link Protection | Reduce Detection Potential (SC-40(2))

Description for Wireless Link Protection | Reduce Detection Potential (SC-40(2))
Implement cryptographic mechanisms to reduce the detection potential of wireless links to [Assignment: organization-defined level of reduction].

Discussion for Wireless Link Protection | Reduce Detection Potential (SC-40(2))
The implementation of cryptographic mechanisms to reduce detection potential is used for covert communications and to protect wireless transmitters from geo-location. It also ensures that the spread spectrum waveforms used to achieve a low probability of detection are not predictable by unauthorized individuals. Mission requirements, projected threats, concept of operations, and applicable laws, executive orders, directives, regulations, policies, and standards determine the levels to which wireless links are undetectable.

Wireless Link Protection | Imitative or Manipulative Communications Deception (SC-40(3))

Description for Wireless Link Protection | Imitative or Manipulative Communications Deception (SC-40(3))
Implement cryptographic mechanisms to identify and reject wireless transmissions that are deliberate attempts to achieve imitative or manipulative communications deception based on signal parameters.

Discussion for Wireless Link Protection | Imitative or Manipulative Communications Deception (SC-40(3))
The implementation of cryptographic mechanisms to identify and reject imitative or manipulative communications ensures that the signal parameters of wireless transmissions are not predictable by unauthorized individuals. Such unpredictability reduces the probability of imitative or manipulative communications deception based on signal parameters alone.

Wireless Link Protection | Signal Parameter Identification (SC-40(4))

Description for Wireless Link Protection | Signal Parameter Identification (SC-40(4))
Implement cryptographic mechanisms to prevent the identification of [Assignment: organization-defined wireless transmitters] by using the transmitter signal parameters.

Discussion for Wireless Link Protection | Signal Parameter Identification (SC-40(4))
The implementation of cryptographic mechanisms to prevent the identification of wireless transmitters protects against the unique identification of wireless transmitters for the purposes of intelligence exploitation by ensuring that anti-fingerprinting alterations to signal parameters are not predictable by unauthorized individuals. It also provides anonymity when required. Radio fingerprinting techniques identify the unique signal parameters of transmitters to fingerprint such transmitters for purposes of tracking and mission or user identification.

Port and I/O Device Access (SC-41)

Description for Port and I/O Device Access (SC-41)
[Selection: Physically; Logically] disable or remove [Assignment: organization-defined connection ports or input/output devices] on the following systems or system components: [Assignment: organization-defined systems or system components].

Discussion for Port and I/O Device Access (SC-41)
Connection ports include Universal Serial Bus (USB), Thunderbolt, and Firewire (IEEE 1394). Input/output (I/O) devices include compact disc and digital versatile disc drives. Disabling or removing such connection ports and I/O devices helps prevent the exfiltration of information from systems and the introduction of malicious code from those ports or devices. Physically disabling or removing ports and/or devices is the stronger action.

Sensor Capability and Data (SC-42)

Description for Sensor Capability and Data (SC-42)
a. Prohibit [Selection (one or more): the use of devices possessing [Assignment: organization-defined environmental sensing capabilities] in [Assignment: organization-defined facilities, areas, or systems]; the remote activation of environmental sensing capabilities on organizational systems or system components with the following exceptions: [Assignment: organization-defined exceptions where remote activation of sensors is allowed]]; and
b. Provide an explicit indication of sensor use to [Assignment: organization-defined group of users].

Discussion for Sensor Capability and Data (SC-42)
Sensor capability and data applies to types of systems or system components characterized as mobile devices, such as cellular telephones, smart phones, and tablets. Mobile devices often include sensors that can collect and record data regarding the environment where the system is in use. Sensors that are embedded within mobile devices include microphones, cameras, Global Positioning System (GPS) mechanisms, and accelerometers. While the sensors on mobiles devices provide an important function, if activated covertly, such devices can potentially provide a means for adversaries to learn valuable information about individuals and organizations. For example, remotely activating the GPS function on a mobile device could provide an adversary with the ability to track the movements of an individual. Organizations may prohibit individuals from bringing cellular telephones or digital cameras into certain designated facilities or controlled areas within facilities where classified information is stored or sensitive conversations are taking place.

Sensor Capability and Data | Reporting to Authorized Individuals or Roles (SC-42(1))

Description for Sensor Capability and Data | Reporting to Authorized Individuals or Roles (SC-42(1))
Verify that the system is configured so that data or information collected by the [Assignment: organization-defined sensors] is only reported to authorized individuals or roles.

Discussion for Sensor Capability and Data | Reporting to Authorized Individuals or Roles (SC-42(1))
In situations where sensors are activated by authorized individuals, it is still possible that the data or information collected by the sensors will be sent to unauthorized entities.

Sensor Capability and Data | Authorized Use (SC-42(2))

Description for Sensor Capability and Data | Authorized Use (SC-42(2))
Employ the following measures so that data or information collected by [Assignment: organization-defined sensors] is only used for authorized purposes: [Assignment: organization-defined measures].

Discussion for Sensor Capability and Data | Authorized Use (SC-42(2))
Information collected by sensors for a specific authorized purpose could be misused for some unauthorized purpose. For example, GPS sensors that are used to support traffic navigation could be misused to track the movements of individuals. Measures to mitigate such activities include additional training to help ensure that authorized individuals do not abuse their authority and, in the case where sensor data is maintained by external parties, contractual restrictions on the use of such data.

Transmission Confidentiality (SC-9)

Description for Transmission Confidentiality (SC-9)
[Withdrawn: Incorporated into SC-8.]

Discussion for Transmission Confidentiality (SC-9)

Sensor Capability and Data | Notice of Collection (SC-42(4))

Description for Sensor Capability and Data | Notice of Collection (SC-42(4))
Employ the following measures to facilitate an individual's awareness that personally identifiable information is being collected by [Assignment: organization-defined sensors]: [Assignment: organization-defined measures].

Discussion for Sensor Capability and Data | Notice of Collection (SC-42(4))
Awareness that organizational sensors are collecting data enables individuals to more effectively engage in managing their privacy. Measures can include conventional written notices and sensor configurations that make individuals directly or indirectly aware through other devices that the sensor is collecting information. The usability and efficacy of the notice are important considerations.

Sensor Capability and Data | Collection Minimization (SC-42(5))

Description for Sensor Capability and Data | Collection Minimization (SC-42(5))
Employ [Assignment: organization-defined sensors] that are configured to minimize the collection of information about individuals that is not needed.

Discussion for Sensor Capability and Data | Collection Minimization (SC-42(5))
Although policies to control for authorized use can be applied to information once it is collected, minimizing the collection of information that is not needed mitigates privacy risk at the system entry point and mitigates the risk of policy control failures. Sensor configurations include the obscuring of human features, such as blurring or pixelating flesh tones.

Usage Restrictions (SC-43)

Description for Usage Restrictions (SC-43)
a. Establish usage restrictions and implementation guidelines for the following system components: [Assignment: organization-defined system components]; and
b. Authorize, monitor, and control the use of such components within the system.

Discussion for Usage Restrictions (SC-43)
Usage restrictions apply to all system components including but not limited to mobile code, mobile devices, wireless access, and wired and wireless peripheral components (e.g., copiers, printers, scanners, optical devices, and other similar technologies). The usage restrictions and implementation guidelines are based on the potential for system components to cause damage to the system and help to ensure that only authorized system use occurs.

Detonation Chambers (SC-44)

Description for Detonation Chambers (SC-44)
Employ a detonation chamber capability within [Assignment: organization-defined system, system component, or location].

Discussion for Detonation Chambers (SC-44)
Detonation chambers, also known as dynamic execution environments, allow organizations to open email attachments, execute untrusted or suspicious applications, and execute Universal Resource Locator requests in the safety of an isolated environment or a virtualized sandbox. Protected and isolated execution environments provide a means of determining whether the associated attachments or applications contain malicious code. While related to the concept of deception nets, the employment of detonation chambers is not intended to maintain a long-term environment in which adversaries can operate and their actions can be observed. Rather, detonation chambers are intended to quickly identify malicious code and either reduce the likelihood that the code is propagated to user environments of operation or prevent such propagation completely.

System Time Synchronization (SC-45)

Description for System Time Synchronization (SC-45)
Synchronize system clocks within and between systems and system components.

Discussion for System Time Synchronization (SC-45)
Time synchronization of system clocks is essential for the correct execution of many system services, including identification and authentication processes that involve certificates and time-of-day restrictions as part of access control. Denial of service or failure to deny expired credentials may result without properly synchronized clocks within and between systems and system components. 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. The granularity of time measurements refers to the degree of synchronization between system clocks and reference clocks, such as clocks synchronizing within hundreds of milliseconds or tens of milliseconds. Organizations may define different time granularities for 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 the capabilities.

System Time Synchronization | Synchronization with Authoritative Time Source (SC-45(1))

Description for System Time Synchronization | Synchronization with Authoritative Time Source (SC-45(1))
(a) Compare the internal system clocks [Assignment: organization-defined frequency] with [Assignment: organization-defined authoritative time source]; and
(b) Synchronize the internal system clocks to the authoritative time source when the time difference is greater than [Assignment: organization-defined time period].

Discussion for System Time Synchronization | Synchronization with Authoritative Time Source (SC-45(1))
Synchronization 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.

System Time Synchronization | Secondary Authoritative Time Source (SC-45(2))

Description for System Time Synchronization | Secondary Authoritative Time Source (SC-45(2))
(a) Identify a secondary authoritative time source that is in a different geographic region than the primary authoritative time source; and
(b) Synchronize the internal system clocks to the secondary authoritative time source if the primary authoritative time source is unavailable.

Discussion for System Time Synchronization | Secondary Authoritative Time Source (SC-45(2))
It may be necessary to employ geolocation information to determine that the secondary authoritative time source is in a different geographic region.

Cross Domain Policy Enforcement (SC-46)

Description for Cross Domain Policy Enforcement (SC-46)
Implement a policy enforcement mechanism [Selection: physically; logically] between the physical and/or network interfaces for the connecting security domains.

Discussion for Cross Domain Policy Enforcement (SC-46)
For logical policy enforcement mechanisms, organizations avoid creating a logical path between interfaces to prevent the ability to bypass the policy enforcement mechanism. For physical policy enforcement mechanisms, the robustness of physical isolation afforded by the physical implementation of policy enforcement to preclude the presence of logical covert channels penetrating the security domain may be needed. Contact ncdsmo@nsa.gov for more information.

Alternate Communications Paths (SC-47)

Description for Alternate Communications Paths (SC-47)
Establish [Assignment: organization-defined alternate communications paths] for system operations organizational command and control.

Discussion for Alternate Communications Paths (SC-47)
An incident, whether adversarial- or nonadversarial-based, can disrupt established communications paths used for system operations and organizational command and control. Alternate communications paths reduce the risk of all communications paths being affected by the same incident. To compound the problem, the inability of organizational officials to obtain timely information about disruptions or to provide timely direction to operational elements after a communications path incident, can impact the ability of the organization to respond to such incidents in a timely manner. Establishing alternate communications paths for command and control purposes, including designating 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.

Sensor Relocation (SC-48)

Description for Sensor Relocation (SC-48)
Relocate [Assignment: organization-defined sensors and monitoring capabilities] to [Assignment: organization-defined locations] under the following conditions or circumstances: [Assignment: organization-defined conditions or circumstances].

Discussion for Sensor Relocation (SC-48)
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 often only has a limited set of monitoring and detection capabilities, and they 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 its chances of achieving its desired goals. By relocating its sensors or monitoring capabilities to new locations, the organization can impede the adversary's ability to achieve its goals. The relocation of the sensors or monitoring capabilities might be done based on threat information that the organization has acquired or randomly to confuse the adversary and make its lateral transition through the system or organization more challenging.

Sensor Relocation | Dynamic Relocation of Sensors or Monitoring Capabilities (SC-48(1))

Description for Sensor Relocation | Dynamic Relocation of Sensors or Monitoring Capabilities (SC-48(1))
Dynamically relocate [Assignment: organization-defined sensors and monitoring capabilities] to [Assignment: organization-defined locations] under the following conditions or circumstances: [Assignment: organization-defined conditions or circumstances].

Discussion for Sensor Relocation | Dynamic Relocation of Sensors or Monitoring Capabilities (SC-48(1))
None.

Hardware-enforced Separation and Policy Enforcement (SC-49)

Description for Hardware-enforced Separation and Policy Enforcement (SC-49)
Implement hardware-enforced separation and policy enforcement mechanisms between [Assignment: organization-defined security domains].

Discussion for Hardware-enforced Separation and Policy Enforcement (SC-49)
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.

Software-enforced Separation and Policy Enforcement (SC-50)

Description for Software-enforced Separation and Policy Enforcement (SC-50)
Implement software-enforced separation and policy enforcement mechanisms between [Assignment: organization-defined security domains].

Discussion for Software-enforced Separation and Policy Enforcement (SC-50)
System owners may require additional strength of mechanism to ensure domain separation and policy enforcement for specific types of threats and environments of operation.

Hardware-based Protection (SC-51)

Description for Hardware-based Protection (SC-51)
a. Employ hardware-based, write-protect for [Assignment: organization-defined system firmware components]; and
b. Implement specific procedures for [Assignment: organization-defined authorized individuals] to manually disable hardware write-protect for firmware modifications and re-enable the write-protect prior to returning to operational mode.

Discussion for Hardware-based Protection (SC-51)
None.

Policy and Procedures (SI-1)

Description for Policy and Procedures (SI-1)
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] system and information integrity policy that:
(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls;
b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and information integrity policy and procedures; and
c. Review and update the current system and information integrity:
1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

Discussion for Policy and Procedures (SI-1)
System and information integrity policy and procedures address the controls in the SI family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of system and information integrity policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, 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. Events that may precipitate an update to system and information integrity policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Flaw Remediation (SI-2)

Description for Flaw Remediation (SI-2)
a. Identify, report, and correct system flaws;
b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
c. Install security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates; and
d. Incorporate flaw remediation into the organizational configuration management process.

Discussion for Flaw Remediation (SI-2)
The need to remediate system flaws applies to all types of software and firmware. Organizations identify systems affected by software flaws, including potential vulnerabilities resulting from those 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.
Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of risk factors, including the security category of the system, the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw), the organizational risk tolerance, the mission supported by the system, or the threat environment. Some types of flaw remediation may require more testing than other types. Organizations determine the type of testing needed for the specific type of flaw remediation activity under consideration and the types of changes that are to be configuration-managed. In some situations, organizations may determine that the testing of software or firmware updates is not necessary or practical, such as when implementing simple malicious code signature updates. In testing decisions, organizations consider whether security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures.

Predictable Failure Prevention | Time Limit on Process Execution Without Supervision (SI-13(2))

Description for Predictable Failure Prevention | Time Limit on Process Execution Without Supervision (SI-13(2))
[Withdrawn: Incorporated into SI-7(16).]

Discussion for Predictable Failure Prevention | Time Limit on Process Execution Without Supervision (SI-13(2))

Flaw Remediation | Automated Flaw Remediation Status (SI-2(2))

Description for Flaw Remediation | Automated Flaw Remediation Status (SI-2(2))
Determine if system components have applicable security-relevant software and firmware updates installed using [Assignment: organization-defined automated mechanisms] [Assignment: organization-defined frequency].

Discussion for Flaw Remediation | Automated Flaw Remediation Status (SI-2(2))
Automated mechanisms can track and determine the status of known flaws for system components.

Flaw Remediation | Time to Remediate Flaws and Benchmarks for Corrective Actions (SI-2(3))

Description for Flaw Remediation | Time to Remediate Flaws and Benchmarks for Corrective Actions (SI-2(3))
(a) Measure the time between flaw identification and flaw remediation; and
(b) Establish the following benchmarks for taking corrective actions: [Assignment: organization-defined benchmarks].

Discussion for Flaw Remediation | Time to Remediate Flaws and Benchmarks for Corrective Actions (SI-2(3))
Organizations determine the time it takes on average to correct system flaws after such flaws have been identified 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.

Flaw Remediation | Automated Patch Management Tools (SI-2(4))

Description for Flaw Remediation | Automated Patch Management Tools (SI-2(4))
Employ automated patch management tools to facilitate flaw remediation to the following system components: [Assignment: organization-defined system components].

Discussion for Flaw Remediation | Automated Patch Management Tools (SI-2(4))
Using automated tools to support patch management helps to ensure the timeliness and completeness of system patching operations.

Flaw Remediation | Automatic Software and Firmware Updates (SI-2(5))

Description for Flaw Remediation | Automatic Software and Firmware Updates (SI-2(5))
Install [Assignment: organization-defined security-relevant software and firmware updates] automatically to [Assignment: organization-defined system components].

Discussion for Flaw Remediation | Automatic Software and Firmware Updates (SI-2(5))
Due to system integrity and availability concerns, organizations consider the methodology used to carry out automatic updates. Organizations balance the need to ensure that the updates are installed as soon as possible with the need to maintain configuration management and control with any mission or operational impacts that automatic updates might impose.

Flaw Remediation | Removal of Previous Versions of Software and Firmware (SI-2(6))

Description for Flaw Remediation | Removal of Previous Versions of Software and Firmware (SI-2(6))
Remove previous versions of [Assignment: organization-defined software and firmware components] after updated versions have been installed.

Discussion for Flaw Remediation | Removal of Previous Versions of Software and Firmware (SI-2(6))
Previous versions of software or firmware components that are not removed from the system after updates have been installed may be exploited by adversaries. Some products may automatically remove previous versions of software and firmware from the system.

Malicious Code Protection (SI-3)

Description for Malicious Code Protection (SI-3)
a. Implement [Selection (one or more): signature based; non-signature based] malicious code protection mechanisms at 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 files from external sources at [Selection (one or more): endpoint; network entry and exit points] as the files are downloaded, opened, or executed in accordance with organizational policy; and
2. [Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]; and send alert to [Assignment: organization-defined personnel or roles] in response to malicious code detection; and
d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.

Discussion for Malicious Code Protection (SI-3)
System entry and exit points include firewalls, remote access servers, workstations, electronic mail servers, web servers, proxy servers, notebook computers, and mobile devices. Malicious code includes viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats contained within compressed or hidden files or hidden in files using techniques 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 insertions occur through the exploitation of system vulnerabilities. A variety of technologies and methods exist to limit or eliminate the effects of malicious code.
Malicious code protection mechanisms include both signature- and nonsignature-based technologies. Nonsignature-based detection mechanisms include artificial intelligence techniques that use heuristics to detect, analyze, and describe the characteristics or behavior of malicious code and to provide controls against such code for which signatures do not yet exist or for which existing signatures may not be effective. Malicious code for which active signatures do not yet exist or may be ineffective includes polymorphic malicious code (i.e., code that changes signatures when it replicates). Nonsignature-based mechanisms also include reputation-based technologies. In addition to the above technologies, pervasive configuration management, comprehensive software integrity controls, and anti-exploitation software may be effective in preventing the execution of unauthorized code. Malicious code may be present in commercial off-the-shelf software as well as

custom-built software and could include logic bombs, backdoors, and other types of attacks that could affect organizational mission and business functions.
In situations where malicious code cannot be detected by detection methods or technologies, organizations rely on other types of controls, including secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to ensure that software does not perform functions other than the functions intended. Organizations may determine that, in response to the detection of malicious code, different actions may be warranted. For example, organizations can define actions in response to malicious code detection during periodic scans, the detection of malicious downloads, or the detection of maliciousness when attempting to open or execute files.

Flaw Remediation | Central Management (SI-2(1))

Description for Flaw Remediation | Central Management (SI-2(1))
[Withdrawn: Incorporated into PL-9.]

Discussion for Flaw Remediation | Central Management (SI-2(1))

Malicious Code Protection | Central Management (SI-3(1))

Description for Malicious Code Protection | Central Management (SI-3(1))
[Withdrawn: Incorporated into PL-9.]

Discussion for Malicious Code Protection | Central Management (SI-3(1))

Malicious Code Protection | Automatic Updates (SI-3(2))

Description for Malicious Code Protection | Automatic Updates (SI-3(2))
[Withdrawn: Incorporated into SI-3.]

Discussion for Malicious Code Protection | Automatic Updates (SI-3(2))

Malicious Code Protection | Updates Only by Privileged Users (SI-3(4))

Description for Malicious Code Protection | Updates Only by Privileged Users (SI-3(4))
Update malicious code protection mechanisms only when directed by a privileged user.

Discussion for Malicious Code Protection | Updates Only by Privileged Users (SI-3(4))
Protection mechanisms for malicious code are typically categorized as security-related software and, as such, are only updated by organizational personnel with appropriate access privileges.

Malicious Code Protection | Non-privileged Users (SI-3(3))

Description for Malicious Code Protection | Non-privileged Users (SI-3(3))
[Withdrawn: Incorporated into AC-6(10).]

Discussion for Malicious Code Protection | Non-privileged Users (SI-3(3))

Malicious Code Protection | Testing and Verification (SI-3(6))

Description for Malicious Code Protection | Testing and Verification (SI-3(6))
(a) Test malicious code protection mechanisms [Assignment: organization-defined frequency] by introducing known benign code into the system; and
(b) Verify that the detection of the code and the associated incident reporting occur.

Discussion for Malicious Code Protection | Testing and Verification (SI-3(6))
None.

Malicious Code Protection | Portable Storage Devices (SI-3(5))

Description for Malicious Code Protection | Portable Storage Devices (SI-3(5))
[Withdrawn: Incorporated into MP-7.]

Discussion for Malicious Code Protection | Portable Storage Devices (SI-3(5))

Malicious Code Protection | Detect Unauthorized Commands (SI-3(8))

Description for Malicious Code Protection | Detect Unauthorized Commands (SI-3(8))
(a) Detect the following unauthorized operating system commands through the kernel application programming interface on [Assignment: organization-defined system hardware components]: [Assignment: organization-defined unauthorized operating system commands]; and
(b) [Selection (one or more): issue a warning; audit the command execution; prevent the execution of the command].

Discussion for Malicious Code Protection | Detect Unauthorized Commands (SI-3(8))
Detecting unauthorized commands can be applied to critical interfaces other than kernel-based interfaces, including interfaces with virtual machines and privileged applications. Unauthorized operating system commands include commands for kernel functions from system processes that are not trusted to initiate such commands as well as commands for kernel functions that are suspicious even though commands of that type are reasonable for processes to initiate. Organizations can define the malicious commands to be detected by a combination of command types, command classes, or specific instances of commands. Organizations can also define hardware components by component type, component, component location in the network, or a combination thereof. Organizations may select different actions for different types, classes, or instances of malicious commands.

Malicious Code Protection | Nonsignature-based Detection (SI-3(7))

Description for Malicious Code Protection | Nonsignature-based Detection (SI-3(7))
[Withdrawn: Incorporated into SI-3.]

Discussion for Malicious Code Protection | Nonsignature-based Detection (SI-3(7))

Malicious Code Protection | Malicious Code Analysis (SI-3(10))

Description for Malicious Code Protection | Malicious Code Analysis (SI-3(10))
(a) Employ the following tools and techniques to analyze the characteristics and behavior of malicious code: [Assignment: organization-defined tools and techniques]; and
(b) Incorporate the results from malicious code analysis into organizational incident response and flaw remediation processes.

Discussion for Malicious Code Protection | Malicious Code Analysis (SI-3(10))
The use of malicious code analysis tools provides organizations with a more in-depth understanding of adversary tradecraft (i.e., tactics, 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 analyses by employing reverse engineering techniques or by monitoring the behavior of executing code.

System Monitoring (SI-4)

Description for System Monitoring (SI-4)
a. Monitor the system to detect:
1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]; and
2. Unauthorized local, network, and remote connections;
b. Identify unauthorized use of the system through the following techniques and methods: [Assignment: organization-defined techniques and methods];
c. Invoke internal monitoring capabilities or deploy monitoring devices:
1. Strategically within the system to collect organization-determined essential information; and
2. At ad hoc locations within the system to track specific types of transactions of interest to the organization;
d. Analyze detected events and anomalies;
e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation;
f. Obtain legal opinion regarding system monitoring activities; and
g. Provide [Assignment: organization-defined system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].

Discussion for System Monitoring (SI-4)
System monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at external interfaces to the system. Internal monitoring includes the observation of events occurring within the system. Organizations monitor systems by observing audit activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions. The monitoring objectives guide and inform the determination of the events. System monitoring capabilities are achieved through a variety of tools and techniques, including intrusion detection and prevention systems, malicious code protection software, scanning tools, audit record monitoring software, and network monitoring software.
Depending on the security architecture, the distribution and configuration of monitoring devices may impact throughput at key internal and external boundaries as well as at other locations across a network due to the introduction of network throughput latency. If throughput management is needed, such devices are strategically located and deployed as part of an established organization-wide security architecture. Strategic locations for monitoring devices include selected perimeter locations and near key servers and server farms that support critical applications. Monitoring devices are typically employed at the managed interfaces associated with controls SC-7 and AC-17. The information collected is a function of

the organizational monitoring objectives and the capability of systems to support such objectives. Specific types of transactions of interest include Hypertext Transfer Protocol (HTTP) traffic that bypasses HTTP proxies. System monitoring is an integral part of organizational continuous monitoring and incident response programs, and output from system monitoring serves as input to those programs. System monitoring requirements, including the need for specific types of system monitoring, may be referenced in other controls (e.g., AC-2g, AC-2(7), AC-2(12)(a), AC-17(1), AU-13, AU-13(1), AU-13(2), CM-3f, CM-6d, MA-3a, MA-4a, SC-5(3)(b), SC-7a, SC-7(24)(b), SC-18b, SC-43b). Adjustments to levels of system monitoring are based on law enforcement information, intelligence information, or other sources of information. The legality of system monitoring activities is based on applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

System Monitoring | System-wide Intrusion Detection System (SI-4(1))

Description for System Monitoring | System-wide Intrusion Detection System (SI-4(1))
Connect and configure individual intrusion detection tools into a system-wide intrusion detection system.

Discussion for System Monitoring | System-wide Intrusion Detection System (SI-4(1))
Linking individual intrusion detection tools into a system-wide intrusion detection system provides additional coverage and effective detection capabilities. The information contained in one intrusion detection tool can be shared widely across the organization, making the system-wide detection capability more robust and powerful.

System Monitoring | Automated Tools and Mechanisms for Real-time Analysis (SI-4(2))

Description for System Monitoring | Automated Tools and Mechanisms for Real-time Analysis (SI-4(2))
Employ automated tools and mechanisms to support near real-time analysis of events.

Discussion for System Monitoring | Automated Tools and Mechanisms for Real-time Analysis (SI-4(2))
Automated tools and mechanisms include host-based, network-based, transport-based, or storage-based event monitoring tools and mechanisms or security information and event management (SIEM) technologies that provide real-time analysis of alerts and notifications generated by organizational systems.
Automated monitoring techniques can create unintended privacy risks because automated controls may connect to external or otherwise unrelated systems. 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 plan.

System Monitoring | Automated Tool and Mechanism Integration (SI-4(3))

Description for System Monitoring | Automated Tool and Mechanism Integration (SI-4(3))
Employ automated tools and mechanisms to integrate intrusion detection tools and mechanisms into access control and flow control mechanisms.

Discussion for System Monitoring | Automated Tool and Mechanism Integration (SI-4(3))
Using automated tools and mechanisms to integrate intrusion detection tools and mechanisms into access and flow control mechanisms facilitates a rapid response to attacks by enabling the reconfiguration of mechanisms in support of attack isolation and elimination.

System Monitoring | Inbound and Outbound Communications Traffic (SI-4(4))

Description for System Monitoring | Inbound and Outbound Communications Traffic (SI-4(4))
(a) Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic;
(b) Monitor inbound and outbound communications traffic [Assignment: organization-defined frequency] for [Assignment: organization-defined unusual or unauthorized activities or conditions].

Discussion for System Monitoring | Inbound and Outbound Communications Traffic (SI-4(4))
Unusual or unauthorized activities or conditions related to system inbound and outbound communications traffic includes internal traffic that indicates the presence of malicious code or unauthorized use of legitimate code or credentials within organizational systems or propagating among system components, signaling to external systems, and the unauthorized exporting of information. Evidence of malicious code or unauthorized use of legitimate code or credentials is used to identify potentially compromised systems or system components.

System Monitoring | System-generated Alerts (SI-4(5))

Description for System Monitoring | System-generated Alerts (SI-4(5))
Alert [Assignment: organization-defined personnel or roles] when the following system-generated indications of compromise or potential compromise occur: [Assignment: organization-defined compromise indicators].

Discussion for System Monitoring | System-generated Alerts (SI-4(5))
Alerts may be generated from a variety of sources, including audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers. Alerts can be automated and may be transmitted telephonically, by electronic mail messages, or by text messaging. Organizational personnel on the alert notification list can include system administrators, mission or business owners, system owners, information owners/stewards, senior agency information security officers, senior agency officials for privacy, system security officers, or privacy officers. In contrast to alerts generated by the system, alerts generated by organizations in SI-4(12) focus on information sources external to the system, such as suspicious activity reports and reports on potential insider threats.

Malicious Code Protection | Authenticate Remote Commands (SI-3(9))

Description for Malicious Code Protection | Authenticate Remote Commands (SI-3(9))
[Withdrawn: Moved to AC-17(10).]

Discussion for Malicious Code Protection | Authenticate Remote Commands (SI-3(9))

System Monitoring | Automated Response to Suspicious Events (SI-4(7))

Description for System Monitoring | Automated Response to Suspicious Events (SI-4(7))
(a) Notify [Assignment: organization-defined incident response personnel (identified by name and/or by role)] of detected suspicious events; and
(b) Take the following actions upon detection: [Assignment: organization-defined least-disruptive actions to terminate suspicious events].

Discussion for System Monitoring | Automated Response to Suspicious Events (SI-4(7))
Least-disruptive actions include initiating requests for human responses.

System Monitoring | Restrict Non-privileged Users (SI-4(6))

Description for System Monitoring | Restrict Non-privileged Users (SI-4(6))
[Withdrawn: Incorporated into AC-6(10).]

Discussion for System Monitoring | Restrict Non-privileged Users (SI-4(6))

System Monitoring | Testing of Monitoring Tools and Mechanisms (SI-4(9))

Description for System Monitoring | Testing of Monitoring Tools and Mechanisms (SI-4(9))
Test intrusion-monitoring tools and mechanisms [Assignment: organization-defined frequency].

Discussion for System Monitoring | Testing of Monitoring Tools and Mechanisms (SI-4(9))
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 depends on the types of tools and mechanisms used by organizations and the methods of deployment.

System Monitoring | Visibility of Encrypted Communications (SI-4(10))

Description for System Monitoring | Visibility of Encrypted Communications (SI-4(10))
Make provisions so that [Assignment: organization-defined encrypted communications traffic] is visible to [Assignment: organization-defined system monitoring tools and mechanisms].

Discussion for System Monitoring | Visibility of Encrypted Communications (SI-4(10))
Organizations balance the need to encrypt communications traffic to protect data confidentiality with the need to maintain visibility into such traffic from a monitoring perspective. Organizations determine whether the visibility requirement applies to internal encrypted traffic, encrypted traffic intended for external destinations, or a subset of the traffic types.

System Monitoring | Analyze Communications Traffic Anomalies (SI-4(11))

Description for System Monitoring | Analyze Communications Traffic Anomalies (SI-4(11))
Analyze outbound communications traffic at the external interfaces to the system and selected [Assignment: organization-defined interior points within the system] to discover anomalies.

Discussion for System Monitoring | Analyze Communications Traffic Anomalies (SI-4(11))
Organization-defined interior points include subnetworks and subsystems. Anomalies within organizational systems include large file transfers, long-time persistent connections, attempts to access information from unexpected locations, the use of unusual protocols and ports, the use of unmonitored network protocols (e.g., IPv6 usage during IPv4 transition), and attempted communications with suspected malicious external addresses.

System Monitoring | Automated Organization-generated Alerts (SI-4(12))

Description for System Monitoring | Automated Organization-generated Alerts (SI-4(12))
Alert [Assignment: organization-defined personnel or roles] using [Assignment: organization-defined automated mechanisms] when the following indications of inappropriate or unusual activities with security or privacy implications occur: [Assignment: organization-defined activities that trigger alerts].

Discussion for System Monitoring | Automated Organization-generated Alerts (SI-4(12))
Organizational personnel on the system alert notification list include system administrators, mission or business owners, system owners, senior agency information security officer, senior agency official for privacy, system security officers, or privacy officers. Automated organization-generated alerts are the security alerts generated by organizations and transmitted using automated means. The sources for organization-generated alerts are focused on other entities such as suspicious activity reports and reports on potential insider threats. In contrast to alerts generated by the organization, alerts generated by the system in SI-4(5) focus on information sources that are internal to the systems, such as audit records.

System Monitoring | Analyze Traffic and Event Patterns (SI-4(13))

Description for System Monitoring | Analyze Traffic and Event Patterns (SI-4(13))
(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.

Discussion for System Monitoring | Analyze Traffic and Event Patterns (SI-4(13))
Identifying and understanding common communications traffic and event patterns help organizations provide useful information to system monitoring devices to more effectively identify suspicious or anomalous traffic and events when they occur. Such information can help reduce the number of false positives and false negatives during system monitoring.

System Monitoring | Wireless Intrusion Detection (SI-4(14))

Description for System Monitoring | Wireless Intrusion Detection (SI-4(14))
Employ a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises or breaches to the system.

Discussion for System Monitoring | Wireless Intrusion Detection (SI-4(14))
Wireless signals may radiate beyond organizational facilities. Organizations proactively search for unauthorized wireless connections, including the conduct of thorough scans for unauthorized wireless access points. Wireless scans are not limited to those areas within facilities containing systems but also include areas outside of facilities to verify that unauthorized wireless access points are not connected to organizational systems.

System Monitoring | Wireless to Wireline Communications (SI-4(15))

Description for System Monitoring | Wireless to Wireline Communications (SI-4(15))
Employ an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wireline networks.

Discussion for System Monitoring | Wireless to Wireline Communications (SI-4(15))
Wireless networks are inherently less secure than wired networks. For example, wireless networks are more susceptible to eavesdroppers or traffic analysis than wireline networks. When wireless to wireline communications exist, the wireless network could become a port of entry into the wired network. Given the greater facility of unauthorized network access via wireless access points compared to unauthorized wired network access from within the physical boundaries of the system, additional monitoring of transitioning traffic between wireless and wired networks may be necessary to detect malicious activities. Employing intrusion detection systems to monitor wireless communications traffic helps to ensure that the traffic does not contain malicious code prior to transitioning to the wireline network.

System Monitoring | Correlate Monitoring Information (SI-4(16))

Description for System Monitoring | Correlate Monitoring Information (SI-4(16))
Correlate information from monitoring tools and mechanisms employed throughout the system.

Discussion for System Monitoring | Correlate Monitoring Information (SI-4(16))
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 unseen attack patterns. Understanding the capabilities and limitations of diverse monitoring tools and mechanisms and how to maximize the use of information generated by those tools and mechanisms can help organizations develop, operate, and maintain effective monitoring programs. The correlation of monitoring information is especially important during the transition from older to newer technologies (e.g., transitioning from IPv4 to IPv6 network protocols).

System Monitoring | Integrated Situational Awareness (SI-4(17))

Description for System Monitoring | Integrated Situational Awareness (SI-4(17))
Correlate information from monitoring physical, cyber, and supply chain activities to achieve integrated, organization-wide situational awareness.

Discussion for System Monitoring | Integrated Situational Awareness (SI-4(17))
Correlating monitoring information from a more diverse set of information sources helps to achieve integrated situational awareness. Integrated situational awareness from a combination of physical, cyber, and supply chain monitoring activities enhances the capability of organizations to more quickly detect sophisticated attacks and investigate the methods and techniques employed to carry out such attacks. In contrast to SI-4(16), which correlates the various cyber monitoring information, integrated situational awareness is intended to correlate monitoring beyond the cyber domain. Correlation of monitoring information from multiple activities may help reveal attacks on organizations that are operating across multiple attack vectors.

System Monitoring | Analyze Traffic and Covert Exfiltration (SI-4(18))

Description for System Monitoring | Analyze Traffic and Covert Exfiltration (SI-4(18))
Analyze outbound communications traffic at external interfaces to the system and at the following interior points to detect covert exfiltration of information: [Assignment: organization-defined interior points within the system].

Discussion for System Monitoring | Analyze Traffic and Covert Exfiltration (SI-4(18))
Organization-defined interior points include subnetworks and subsystems. Covert means that can be used to exfiltrate information include steganography.

System Monitoring | Risk for Individuals (SI-4(19))

Description for System Monitoring | Risk for Individuals (SI-4(19))
Implement [Assignment: organization-defined additional monitoring] of individuals who have been identified by [Assignment: organization-defined sources] as posing an increased level of risk.

Discussion for System Monitoring | Risk for Individuals (SI-4(19))
Indications of increased risk from individuals can be obtained from different sources, including personnel records, intelligence agencies, law enforcement organizations, and other sources. The monitoring of individuals is coordinated with the management, legal, security, privacy, and human resource officials who conduct such monitoring. Monitoring is conducted in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

System Monitoring | Privileged Users (SI-4(20))

Description for System Monitoring | Privileged Users (SI-4(20))
Implement the following additional monitoring of privileged users: [Assignment: organization-defined additional monitoring].

Discussion for System Monitoring | Privileged Users (SI-4(20))
Privileged users have access to more sensitive information, including security-related information, than the 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.

System Monitoring | Probationary Periods (SI-4(21))

Description for System Monitoring | Probationary Periods (SI-4(21))
Implement the following additional monitoring of individuals during [Assignment: organization-defined probationary period]: [Assignment: organization-defined additional monitoring].

Discussion for System Monitoring | Probationary Periods (SI-4(21))
During probationary periods, employees do not have permanent employment status within organizations. Without such status or access to information that is resident on the system, additional monitoring can help identify any potentially malicious activity or inappropriate behavior.

System Monitoring | Unauthorized Network Services (SI-4(22))

Description for System Monitoring | Unauthorized Network Services (SI-4(22))
(a) Detect network services that have not been authorized or approved by [Assignment: organization-defined authorization or approval processes]; and
(b) [Selection (one or more): Audit; Alert [Assignment: organization-defined personnel or roles]] when detected.

Discussion for System Monitoring | Unauthorized Network Services (SI-4(22))
Unauthorized or unapproved network services include services in service-oriented architectures that lack organizational verification or validation and may therefore be unreliable or serve as malicious rogues for valid services.

System Monitoring | Host-based Devices (SI-4(23))

Description for System Monitoring | Host-based Devices (SI-4(23))
Implement the following host-based monitoring mechanisms at [Assignment: organization-defined system components]: [Assignment: organization-defined host-based monitoring mechanisms].

Discussion for System Monitoring | Host-based Devices (SI-4(23))
Host-based monitoring collects information about the host (or system in which it resides). System components in which host-based monitoring can be implemented include servers, notebook computers, and mobile devices. Organizations may

consider employing host-based monitoring mechanisms from multiple product developers or vendors.

System Monitoring | Indicators of Compromise (SI-4(24))

Description for System Monitoring | Indicators of Compromise (SI-4(24))
Discover, collect, and distribute to [Assignment: organization-defined personnel or roles], indicators of compromise provided by [Assignment: organization-defined sources].

Discussion for System Monitoring | Indicators of Compromise (SI-4(24))
Indicators of compromise (IOC) 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 traffic include Universal Resource Locator or protocol elements that indicate 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 exploit or attack. Threat indicators, signatures, tactics, techniques, procedures, and other indicators of compromise may be available via government and non-government cooperatives, including the Forum of Incident Response and Security Teams, the United States Computer Emergency Readiness Team, the Defense Industrial Base Cybersecurity Information Sharing Program, and the CERT Coordination Center.

System Monitoring | Optimize Network Traffic Analysis (SI-4(25))

Description for System Monitoring | Optimize Network Traffic Analysis (SI-4(25))
Provide visibility into network traffic at external and key internal system interfaces to optimize the effectiveness of monitoring devices.

Discussion for System Monitoring | Optimize Network Traffic Analysis (SI-4(25))
Encrypted traffic, asymmetric routing architectures, capacity and latency limitations, and transitioning from older to newer technologies (e.g., IPv4 to IPv6 network protocol transition) may result in blind spots for organizations when analyzing network traffic. Collecting, decrypting, pre-processing, and distributing only relevant traffic to monitoring devices can streamline the efficiency and use of devices and optimize traffic analysis.

Security Alerts, Advisories, and Directives (SI-5)

Description for Security Alerts, Advisories, and Directives (SI-5)
a. Receive system security alerts, advisories, and directives from [Assignment: organization-defined external organizations] on an ongoing basis;
b. Generate internal security alerts, advisories, and directives as deemed necessary;
c. Disseminate security alerts, advisories, and directives to: [Selection (one or more): [Assignment: organization-defined personnel or roles]; [Assignment: organization-defined elements within the organization]; [Assignment: organization-defined external organizations]]; and
d. Implement security directives in accordance with established time frames, or notify the issuing organization of the degree of noncompliance.

Discussion for Security Alerts, Advisories, and Directives (SI-5)
The Cybersecurity and Infrastructure Security Agency (CISA) generates security alerts and advisories to maintain situational awareness throughout the Federal Government. Security directives are issued by OMB or other designated organizations with the responsibility and authority to issue such directives. Compliance with security directives is essential due to the critical nature of many of these directives and the potential (immediate) adverse effects on organizational operations and assets, individuals, other organizations, and the Nation should the directives not be implemented in a timely manner. External organizations include supply chain partners, external mission or business partners, external service providers, and other peer or supporting organizations.

Security Alerts, Advisories, and Directives | Automated Alerts and Advisories (SI-5(1))

Description for Security Alerts, Advisories, and Directives | Automated Alerts and Advisories (SI-5(1))
Broadcast security alert and advisory information throughout the organization using [Assignment: organization-defined automated mechanisms].

Discussion for Security Alerts, Advisories, and Directives | Automated Alerts and Advisories (SI-5(1))
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 interest in the success of organizational mission 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 risk, including the governance level, mission and business process level, and the information system level.

Security and Privacy Function Verification (SI-6)

Description for Security and Privacy Function Verification (SI-6)
a. Verify the correct operation of [Assignment: organization-defined security and privacy functions];
b. Perform the verification of the functions specified in SI-6a [Selection (one or more): [Assignment: organization-defined system transitional states]; upon command by user with appropriate privilege; [Assignment: organization-defined frequency]];
c. Alert [Assignment: organization-defined personnel or roles] to failed security and privacy verification tests; and
d. [Selection (one or more): Shut the system down; Restart the system; [Assignment: organization-defined alternative action(s)]] when anomalies are discovered.

Discussion for Security and Privacy Function Verification (SI-6)
Transitional states for systems include system startup, restart, shutdown, and abort. System notifications include hardware indicator lights, electronic alerts to system administrators, and messages to local computer consoles. In contrast to security function verification, privacy function verification ensures that privacy functions operate as expected and are approved by the senior agency official for privacy or that privacy attributes are applied or used as expected.

System Monitoring | Protection of Monitoring Information (SI-4(8))

Description for System Monitoring | Protection of Monitoring Information (SI-4(8))
[Withdrawn: Incorporated into SI-4.]

Discussion for System Monitoring | Protection of Monitoring Information (SI-4(8))

Security and Privacy Function Verification | Automation Support for Distributed Testing (SI-6(2))

Description for Security and Privacy Function Verification | Automation Support for Distributed Testing (SI-6(2))
Implement automated mechanisms to support the management of distributed security and privacy function testing.

Discussion for Security and Privacy Function Verification | Automation Support for Distributed Testing (SI-6(2))
The use of automated mechanisms to support the management of distributed function testing helps to ensure the integrity, timeliness, completeness, and efficacy of such testing.

Security and Privacy Function Verification | Report Verification Results (SI-6(3))

Description for Security and Privacy Function Verification | Report Verification Results (SI-6(3))
Report the results of security and privacy function verification to [Assignment: organization-defined personnel or roles].

Discussion for Security and Privacy Function Verification | Report Verification Results (SI-6(3))
Organizational personnel with potential interest in the results of the verification of security and privacy functions include systems security officers, senior agency information security officers, and senior agency officials for privacy.

Software, Firmware, and Information Integrity (SI-7)

Description for Software, Firmware, and Information Integrity (SI-7)
a. Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: [Assignment: organization-defined software, firmware, and information]; and
b. Take the following actions when unauthorized changes to the software, firmware, and information are detected: [Assignment: organization-defined actions].

Discussion for Software, Firmware, and Information Integrity (SI-7)
Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity. Software includes operating systems (with key internal components, such as kernels or drivers), middleware, and applications. Firmware interfaces include Unified Extensible Firmware Interface (UEFI) and Basic Input/Output System (BIOS). Information includes personally identifiable information and metadata that contains security and privacy attributes associated

with information. Integrity-checking mechanisms—including parity checks, cyclical redundancy checks, cryptographic hashes, and associated tools—can automatically monitor the integrity of systems and hosted applications.

Software, Firmware, and Information Integrity | Integrity Checks (SI-7(1))

Description for Software, Firmware, and Information Integrity | Integrity Checks (SI-7(1))
Perform an integrity check of [Assignment: organization-defined software, firmware, and information] [Selection (one or more): at startup; at [Assignment: organization-defined transitional states or security-relevant events]; [Assignment: organization-defined frequency]].

Discussion for Software, Firmware, and Information Integrity | Integrity Checks (SI-7(1))
Security-relevant events include the identification of new threats to which organizational systems are susceptible and the installation of new hardware, software, or firmware. Transitional states include system startup, restart, shutdown, and abort.

Software, Firmware, and Information Integrity | Automated Notifications of Integrity Violations (SI-7(2))

Description for Software, Firmware, and Information Integrity | Automated Notifications of Integrity Violations (SI-7(2))
Employ automated tools that provide notification to [Assignment: organization-defined personnel or roles] upon discovering discrepancies during integrity verification.

Discussion for Software, Firmware, and Information Integrity | Automated Notifications of Integrity Violations (SI-7(2))
The employment of automated tools to report system and information integrity violations and to notify organizational personnel in a timely matter is essential to effective risk response. Personnel with an interest in system and information integrity violations include mission and business owners, system owners, senior agency information security official, senior agency official for privacy, system administrators, software developers, systems integrators, information security officers, and privacy officers.

Software, Firmware, and Information Integrity | Centrally Managed Integrity Tools (SI-7(3))

Description for Software, Firmware, and Information Integrity | Centrally Managed Integrity Tools (SI-7(3))
Employ centrally managed integrity verification tools.

Discussion for Software, Firmware, and Information Integrity | Centrally Managed Integrity Tools (SI-7(3))
Centrally managed integrity verification tools provides greater consistency in the application of such tools and can facilitate more comprehensive coverage of integrity verification actions.

Security and Privacy Function Verification | Notification of Failed Security Tests (SI-6(1))

Description for Security and Privacy Function Verification | Notification of Failed Security Tests (SI-6(1))
[Withdrawn: Incorporated into SI-6.]

Discussion for Security and Privacy Function Verification | Notification of Failed Security Tests (SI-6(1))

Software, Firmware, and Information Integrity | Automated Response to Integrity Violations (SI-7(5))

Description for Software, Firmware, and Information Integrity | Automated Response to Integrity Violations (SI-7(5))
Automatically [Selection (one or more): shut the system down; restart the system; implement [Assignment: organization-defined controls]] when integrity violations are discovered.

Discussion for Software, Firmware, and Information Integrity | Automated Response to Integrity Violations (SI-7(5))
Organizations may define different integrity-checking responses by type of information, specific information, or a combination of both. Types of information include firmware, software, and user data. Specific information includes boot firmware for certain types of machines. The automatic implementation of controls within organizational systems includes reversing the changes, halting the system, or triggering audit alerts when unauthorized modifications to critical security files occur.

Software, Firmware, and Information Integrity | Cryptographic Protection (SI-7(6))

Description for Software, Firmware, and Information Integrity | Cryptographic Protection (SI-7(6))
Implement cryptographic mechanisms to detect unauthorized changes to software, firmware, and information.

Discussion for Software, Firmware, and Information Integrity | Cryptographic Protection (SI-7(6))
Cryptographic mechanisms used to protect integrity include digital signatures and the computation 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 that employ cryptographic mechanisms also consider cryptographic key management solutions.

Software, Firmware, and Information Integrity | Integration of Detection and Response (SI-7(7))

Description for Software, Firmware, and Information Integrity | Integration of Detection and Response (SI-7(7))
Incorporate the detection of the following unauthorized changes into the organizational incident response capability: [Assignment: organization-defined security-relevant changes to the system].

Discussion for Software, Firmware, and Information Integrity | Integration of Detection and Response (SI-7(7))
Integrating detection and response helps to ensure that detected events are tracked, monitored, corrected, and available for historical purposes. Maintaining historical records is important for being able to identify and discern adversary actions over an extended time period and for possible legal actions. Security-relevant changes include unauthorized changes to established configuration settings or the unauthorized elevation of system privileges.

Software, Firmware, and Information Integrity | Auditing Capability for Significant Events (SI-7(8))

Description for Software, Firmware, and Information Integrity | Auditing Capability for Significant Events (SI-7(8))
Upon detection of a potential integrity violation, provide the capability to audit the event and initiate the following actions: [Selection (one or more): generate an audit record; alert current user; alert [Assignment: organization-defined personnel or roles]; [Assignment: organization-defined other actions]].

Discussion for Software, Firmware, and Information Integrity | Auditing Capability for Significant Events (SI-7(8))
Organizations select response actions based on types of software, specific software, or information for which there are potential integrity violations.

Software, Firmware, and Information Integrity | Verify Boot Process (SI-7(9))

Description for Software, Firmware, and Information Integrity | Verify Boot Process (SI-7(9))
Verify the integrity of the boot process of the following system components: [Assignment: organization-defined system components].

Discussion for Software, Firmware, and Information Integrity | Verify Boot Process (SI-7(9))
Ensuring the integrity of boot processes is critical to starting system components in known, trustworthy states. Integrity verification mechanisms provide a level of assurance that only trusted code is executed during boot processes.

Software, Firmware, and Information Integrity | Protection of Boot Firmware (SI-7(10))

Description for Software, Firmware, and Information Integrity | Protection of Boot Firmware (SI-7(10))
Implement the following mechanisms to protect the integrity of boot firmware in [Assignment: organization-defined system components]: [Assignment: organization-defined mechanisms].

Discussion for Software, Firmware, and Information Integrity | Protection of Boot Firmware (SI-7(10))
Unauthorized modifications to boot firmware may indicate a sophisticated, targeted attack. These types of targeted attacks can result in a permanent denial of service or a persistent malicious code presence. These situations can occur if the firmware is corrupted or if the malicious code is embedded within the firmware. System components can protect the integrity of boot firmware in organizational systems by verifying the integrity and authenticity of all updates to the firmware prior to applying changes to the system component and preventing unauthorized processes from modifying the boot firmware.

Software, Firmware, and Information Integrity | Confined Environments with Limited Privileges (SI-7(11))

Description for Software, Firmware, and Information Integrity | Confined Environments with Limited Privileges (SI-7(11))
[Withdrawn: Moved to CM-7(6).]

Discussion for Software, Firmware, and Information Integrity | Confined Environments with Limited Privileges (SI-7(11))

Software, Firmware, and Information Integrity | Integrity Verification (SI-7(12))

Description for Software, Firmware, and Information Integrity | Integrity Verification (SI-7(12))
Require that the integrity of the following user-installed software be verified prior to execution: [Assignment: organization-defined user-installed software].

Discussion for Software, Firmware, and Information Integrity | Integrity Verification (SI-7(12))
Organizations verify the integrity of user-installed software prior to execution to reduce the likelihood of executing malicious code or programs that contains errors from unauthorized modifications. Organizations consider the practicality of approaches to verifying software integrity, including the availability of trustworthy checksums from software developers and vendors.

Software, Firmware, and Information Integrity | Code Execution in Protected Environments (SI-7(13))

Description for Software, Firmware, and Information Integrity | Code Execution in Protected Environments (SI-7(13))
[Withdrawn: Moved to CM-7(7).]

Discussion for Software, Firmware, and Information Integrity | Code Execution in Protected Environments (SI-7(13))

Software, Firmware, and Information Integrity | Binary or Machine Executable Code (SI-7(14))

Description for Software, Firmware, and Information Integrity | Binary or Machine Executable Code (SI-7(14))
[Withdrawn: Moved to CM-7(8).]

Discussion for Software, Firmware, and Information Integrity | Binary or Machine Executable Code (SI-7(14))

Software, Firmware, and Information Integrity | Code Authentication (SI-7(15))

Description for Software, Firmware, and Information Integrity | Code Authentication (SI-7(15))
Implement cryptographic mechanisms to authenticate the following software or firmware components prior to installation: [Assignment: organization-defined software or firmware components].

Discussion for Software, Firmware, and Information Integrity | Code Authentication (SI-7(15))
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 that employ cryptographic mechanisms also consider cryptographic key management solutions.

Software, Firmware, and Information Integrity | Time Limit on Process Execution Without Supervision (SI-7(16))

Description for Software, Firmware, and Information Integrity | Time Limit on Process Execution Without Supervision (SI-7(16))
Prohibit processes from executing without supervision for more than [Assignment: organization-defined time period].

Discussion for Software, Firmware, and Information Integrity | Time Limit on Process Execution Without Supervision (SI-7(16))
Placing a time limit on process execution without supervision is intended to apply to 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, and manual oversight and response when system process anomalies occur.

Software, Firmware, and Information Integrity | Runtime Application Self-protection (SI-7(17))

Description for Software, Firmware, and Information Integrity | Runtime Application Self-protection (SI-7(17))
Implement [Assignment: organization-defined controls] for application self-protection at runtime.

Discussion for Software, Firmware, and Information Integrity | Runtime Application Self-protection (SI-7(17))
Runtime application self-protection employs runtime instrumentation to detect and block the exploitation of software vulnerabilities by taking advantage of information from the software in execution. Runtime exploit prevention differs from traditional perimeter-based protections such as guards and firewalls which can only detect and block attacks by using network information without contextual awareness. Runtime application self-protection technology can reduce the susceptibility of software to attacks by monitoring its inputs and blocking those inputs that could allow attacks. It can also help protect the runtime environment from unwanted changes and tampering. When a threat is detected, runtime application self-protection technology can prevent exploitation and take other actions (e.g., sending a warning message to the user, terminating the user's session, terminating the application, or sending an alert to organizational personnel). Runtime application self-protection solutions can be deployed in either a monitor or protection mode.

Spam Protection (SI-8)

Description for Spam Protection (SI-8)
a. Employ spam protection mechanisms at system entry and exit 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.

Discussion for Spam Protection (SI-8)
System entry and exit 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 accesses. Spam protection mechanisms include signature definitions.

Software, Firmware, and Information Integrity | Tamper-evident Packaging (SI-7(4))

Description for Software, Firmware, and Information Integrity | Tamper-evident Packaging (SI-7(4))
[Withdrawn: Incorporated into SR-9.]

Discussion for Software, Firmware, and Information Integrity | Tamper-evident Packaging (SI-7(4))

Spam Protection | Automatic Updates (SI-8(2))

Description for Spam Protection | Automatic Updates (SI-8(2))
Automatically update spam protection mechanisms [Assignment: organization-defined frequency].

Discussion for Spam Protection | Automatic Updates (SI-8(2))
Using automated mechanisms to update spam protection mechanisms helps to ensure that updates occur on a regular basis and provide the latest content and protection capabilities.

Spam Protection | Continuous Learning Capability (SI-8(3))

Description for Spam Protection | Continuous Learning Capability (SI-8(3))
Implement spam protection mechanisms with a learning capability to more effectively identify legitimate communications traffic.

Discussion for Spam Protection | Continuous Learning Capability (SI-8(3))
Learning mechanisms include Bayesian filters that respond to user inputs that identify specific traffic as spam or legitimate by updating algorithm parameters and thereby more accurately separating types of traffic.

Spam Protection | Central Management (SI-8(1))

Description for Spam Protection | Central Management (SI-8(1))
[Withdrawn: Incorporated into PL-9.]

Discussion for Spam Protection | Central Management (SI-8(1))

Information Input Validation (SI-10)

Description for Information Input Validation (SI-10)
Check the validity of the following information inputs: [Assignment: organization-defined information inputs to the system].

Discussion for Information Input Validation (SI-10)
Checking the valid syntax and semantics of system inputs—including character set, length, numerical range, and acceptable values—verifies that inputs match specified definitions for format and content. For example, if the organization specifies that numerical values between 1-100 are the only acceptable inputs for a field in a given application, inputs of 387, abc, or %K% are invalid inputs and are not accepted as input to the system. Valid inputs are likely to vary from field to field within a software application. Applications typically follow well-defined protocols that use structured messages (i.e., commands or queries) to communicate between software modules or system components. Structured messages can contain raw or unstructured data interspersed with metadata or control information. If software applications use attacker-supplied inputs to construct structured messages without properly encoding such messages, then the attacker could insert malicious commands or special characters that can cause the data to be interpreted as control information or metadata. Consequently, the module or component that receives the corrupted output will perform the wrong operations or otherwise interpret the data incorrectly. Prescreening inputs prior to passing them to interpreters prevents the content from being unintentionally interpreted as commands. Input validation ensures accurate and correct inputs and prevents attacks such as cross-site scripting and a variety of injection attacks.

Information Input Validation | Manual Override Capability (SI-10(1))

Description for Information Input Validation | Manual Override Capability (SI-10(1))
(a) Provide a manual override capability for input validation of the following information inputs: [Assignment: organization-defined inputs defined in the base control (SI-10)];
(b) Restrict the use of the manual override capability to only [Assignment: organization-defined authorized individuals]; and
(c) Audit the use of the manual override capability.

Discussion for Information Input Validation | Manual Override Capability (SI-10(1))
In certain situations, such as during events that are defined in contingency plans, a manual override capability for input validation may be needed. Manual overrides are used only in limited circumstances and with the inputs defined by the organization.

Information Input Validation | Review and Resolve Errors (SI-10(2))

Description for Information Input Validation | Review and Resolve Errors (SI-10(2))
Review and resolve input validation errors within [Assignment: organization-defined time period].

Discussion for Information Input Validation | Review and Resolve Errors (SI-10(2))
Resolution of input validation errors includes correcting systemic causes of errors and resubmitting transactions with corrected input. Input validation errors are those related to the information inputs defined by the organization in the base control (SI-10).

Information Input Validation | Predictable Behavior (SI-10(3))

Description for Information Input Validation | Predictable Behavior (SI-10(3))
Verify that the system behaves in a predictable and documented manner when invalid inputs are received.

Discussion for Information Input Validation | Predictable Behavior (SI-10(3))
A common vulnerability in organizational systems is unpredictable behavior when invalid inputs are received. Verification of system predictability helps ensure that the system behaves as expected when invalid inputs are received. This occurs by specifying system responses that allow the system to transition to known states without adverse, unintended side effects. The invalid inputs are those related to the information inputs defined by the organization in the base control (SI-10).

Information Input Validation | Timing Interactions (SI-10(4))

Description for Information Input Validation | Timing Interactions (SI-10(4))
Account for timing interactions among system components in determining appropriate responses for invalid inputs.

Discussion for Information Input Validation | Timing Interactions (SI-10(4))
In addressing invalid system inputs received across protocol interfaces, timing interactions become relevant, where one protocol needs to consider the impact of the error response on other protocols in the protocol stack. For example, 802.11 standard wireless network protocols do not interact well with Transmission Control Protocols (TCP) when packets are dropped (which could be due to invalid packet input). TCP assumes packet losses are due to congestion, while packets lost over 802.11 links are typically dropped due to noise or collisions on the link. If TCP makes a congestion response, it takes the wrong action in response to a collision event. Adversaries may be able to use what appear to be acceptable individual behaviors of the protocols in concert to achieve adverse effects through suitable construction of invalid input. The invalid inputs are those related to the information inputs defined by the organization in the base control (SI-10).

Information Input Validation | Restrict Inputs to Trusted Sources and Approved Formats (SI-10(5))

Description for Information Input Validation | Restrict Inputs to Trusted Sources and Approved Formats (SI-10(5))
Restrict the use of information inputs to [Assignment: organization-defined trusted sources] and/or [Assignment: organization-defined formats].

Discussion for Information Input Validation | Restrict Inputs to Trusted Sources and Approved Formats (SI-10(5))
Restricting the use of inputs to trusted sources and in trusted formats applies the concept of authorized or permitted software to information inputs. Specifying known trusted sources for information inputs and acceptable formats for such inputs can reduce the probability of malicious activity. The information inputs are those defined by the organization in the base control (SI-10).

Information Input Validation | Injection Prevention (SI-10(6))

Description for Information Input Validation | Injection Prevention (SI-10(6))
Prevent untrusted data injections.

Discussion for Information Input Validation | Injection Prevention (SI-10(6))
Untrusted data injections may be prevented using a parameterized interface or output escaping (output encoding). Parameterized interfaces separate data from code so that injections of malicious or unintended data cannot change the semantics of commands being sent. Output escaping uses specified characters to inform the interpreter's parser whether data is trusted. Prevention of untrusted data injections are with respect to the information inputs defined by the organization in the base control (SI-10).

Error Handling (SI-11)

Description for Error Handling (SI-11)
a. Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited; and
b. Reveal error messages only to [Assignment: organization-defined personnel or roles].

Discussion for Error Handling (SI-11)
Organizations consider the structure and 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 logon attempts with passwords mistakenly entered as the username; mission or business information that can be derived from, if not stated explicitly by, 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.

Information Management and Retention (SI-12)

Description for Information Management and Retention (SI-12)
Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines and operational requirements.

Discussion for Information Management and Retention (SI-12)
Information management and retention requirements cover the full life cycle of information, in some cases extending beyond system disposal. Information to be retained may also include policies, procedures, plans, reports, data output from control implementation, and other types of administrative information. The National Archives and Records Administration (NARA) provides federal policy and guidance on records retention and schedules. If organizations have a records management office, consider coordinating with records management personnel. Records produced from the output of implemented controls that may require management and retention include, but are not limited to: All XX-1, AC-6(9), AT-4, AU-12, CA-2, CA-3, CA-5, CA-6, CA-7, CA-8, CA-9, CM-2, CM-3, CM-4, CM-6, CM-8, CM-9, CM-12, CM-13, CP-2, IR-6, IR-8, MA-2, MA-4, PE-2, PE-8, PE-16, PE-17, PL-2, PL-4, PL-7, PL-8, PM-5, PM-8, PM-9, PM-18, PM-21, PM-27, PM-28, PM-30, PM-31, PS-2, PS-6, PS-7, PT-2, PT-3, PT-7, RA-2, RA-3, RA-5, RA-8, SA-4, SA-5, SA-8, SA-10, SI-4, SR-2, SR-4, SR-8.

Information Management and Retention | Limit Personally Identifiable Information Elements (SI-12(1))

Description for Information Management and Retention | Limit Personally Identifiable Information Elements (SI-12(1))
Limit personally identifiable information being processed in the information life cycle to the following elements of personally identifiable information: [Assignment: organization-defined elements of personally identifiable information].

Discussion for Information Management and Retention | Limit Personally Identifiable Information Elements (SI-12(1))
Limiting the use of personally identifiable information throughout the information life cycle when the information is not needed for operational purposes helps to reduce the level of privacy risk created by a system. The information life cycle includes information creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposition. Risk assessments as well as applicable laws, regulations, and policies can provide useful inputs to determining which elements of personally identifiable information may create risk.

Information Management and Retention | Minimize Personally Identifiable Information in Testing, Training, and Research (SI-12(2))

Description for Information Management and Retention | Minimize Personally Identifiable Information in Testing, Training, and Research (SI-12(2))
Use the following techniques to minimize the use of personally identifiable information for research, testing, or training: [Assignment: organization-defined techniques].

Discussion for Information Management and Retention | Minimize Personally Identifiable Information in Testing, Training, and Research (SI-12(2))
Organizations can minimize the risk to an individual's privacy by employing techniques such as de-identification or synthetic data. Limiting the use of personally identifiable information throughout the information life cycle when the information is not needed for research, testing, or training helps reduce the level of privacy risk created by a system. Risk assessments as well as applicable laws, regulations, and policies can provide useful inputs to determining the techniques to use and when to use them.

Information Management and Retention | Information Disposal (SI-12(3))

Description for Information Management and Retention | Information Disposal (SI-12(3))
Use the following techniques to dispose of, destroy, or erase information following the retention period: [Assignment: organization-defined techniques].

Discussion for Information Management and Retention | Information Disposal (SI-12(3))
Organizations can minimize both security and privacy risks by disposing of information when it is no longer needed. The disposal or destruction of information applies to originals as well as copies and archived records, including system logs that may contain personally identifiable information.

Predictable Failure Prevention (SI-13)

Description for Predictable Failure Prevention (SI-13)
a. Determine mean time to failure (MTTF) for the following system components in specific environments of operation: [Assignment: organization-defined system components]; 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].

Discussion for Predictable Failure Prevention (SI-13)
While MTTF is primarily a reliability issue, predictable failure prevention is intended to address potential failures of system components that provide security capabilities. Failure rates reflect installation-specific consideration rather than the industry-average. Organizations define the criteria for the substitution of system components based on the MTTF value with consideration for the potential harm from component failures. The transfer of responsibilities between active and standby components does not compromise safety, operational readiness, or security capabilities. The preservation of system state variables is also critical to help ensure a successful transfer process. Standby components remain available at all times except for maintenance issues or recovery failures in progress.

Predictable Failure Prevention | Transferring Component Responsibilities (SI-13(1))

Description for Predictable Failure Prevention | Transferring Component Responsibilities (SI-13(1))
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.

Discussion for Predictable Failure Prevention | Transferring Component Responsibilities (SI-13(1))
Transferring primary system component responsibilities to other substitute components prior to primary component failure is important to reduce the risk of degraded or debilitated mission or business functions. Making such transfers based on a percentage of mean time to failure allows organizations to be proactive based on their risk tolerance. However, the premature replacement of system components can result in the increased cost of system operations.

Information Input Restrictions (SI-9)

Description for Information Input Restrictions (SI-9)
[Withdrawn: Incorporated into AC-2, AC-3, AC-5, and AC-6.]

Discussion for Information Input Restrictions (SI-9)

Predictable Failure Prevention | Manual Transfer Between Components (SI-13(3))

Description for Predictable Failure Prevention | Manual Transfer Between Components (SI-13(3))
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.

Discussion for Predictable Failure Prevention | Manual Transfer Between Components (SI-13(3))
For example, if the MTTF for a system component is 100 days and the MTTF percentage defined by the organization is 90 percent, the manual transfer would occur after 90 days.

Predictable Failure Prevention | Standby Component Installation and Notification (SI-13(4))

Description for Predictable Failure Prevention | Standby Component Installation and Notification (SI-13(4))
If system component failures are detected:
(a) Ensure that the standby components are successfully and transparently installed within [Assignment: organization-defined time period]; and
(b) [Selection (one or more): Activate [Assignment: organization-defined alarm]; Automatically shut down the system; [Assignment: organization-defined action]].

Discussion for Predictable Failure Prevention | Standby Component Installation and Notification (SI-13(4))
Automatic or manual transfer of components from standby to active mode can occur upon the detection of component failures.

Predictable Failure Prevention | Failover Capability (SI-13(5))

Description for Predictable Failure Prevention | Failover Capability (SI-13(5))
Provide [Selection: real-time; near real-time] [Assignment: organization-defined failover capability] for the system.

Discussion for Predictable Failure Prevention | Failover Capability (SI-13(5))
Failover refers to the automatic switchover to an alternate system upon the failure of the primary system. Failover capability includes incorporating mirrored system operations at alternate processing sites or periodic data mirroring at regular intervals defined by the recovery time periods of organizations.

Non-persistence (SI-14)

Description for Non-persistence (SI-14)
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 of use; periodically at [Assignment: organization-defined frequency]].

Discussion for Non-persistence (SI-14)
Implementation of non-persistent components and services mitigates risk from advanced persistent threats (APTs) by reducing the targeting capability of adversaries (i.e., window of opportunity and available attack surface) to initiate and complete attacks. By implementing the concept of non-persistence for selected system components, organizations can provide a trusted, known state computing resource for a specific time period that does not give adversaries sufficient time to exploit vulnerabilities in organizational systems or operating environments. Since the APT is a high-end, sophisticated threat with regard to capability, intent, and targeting, organizations assume that over 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 the end of sessions. Non-persistence increases the work factor of adversaries attempting to compromise or breach organizational systems.
Non-persistence can be achieved by refreshing system components, periodically reimaging components, or 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 intended impact of attacks, but not with such frequency that it makes the system unstable. Refreshes of critical components and services may be done periodically to hinder the ability of adversaries to exploit optimum windows of vulnerabilities.

Non-persistence | Refresh from Trusted Sources (SI-14(1))

Description for Non-persistence | Refresh from Trusted Sources (SI-14(1))
Obtain software and data employed during system component and service refreshes from the following trusted sources: [Assignment: organization-defined trusted sources].

Discussion for Non-persistence | Refresh from Trusted Sources (SI-14(1))
Trusted sources include software and data from write-once, read-only media or from selected offline secure storage facilities.

Non-persistence | Non-persistent Information (SI-14(2))

Description for Non-persistence | Non-persistent Information (SI-14(2))
(a) [Selection: Refresh [Assignment: organization-defined information][Assignment: organization-defined frequency]; Generate [Assignment: organization-defined information] on demand]; and
(b) Delete information when no longer needed.

Discussion for Non-persistence | Non-persistent Information (SI-14(2))
Retaining information longer than is needed makes the information a potential target for advanced adversaries searching for high value assets to compromise through unauthorized disclosure, unauthorized modification, or exfiltration. For system-related information, unnecessary retention provides advanced adversaries information that can assist in their reconnaissance and lateral movement through the system.

Non-persistence | Non-persistent Connectivity (SI-14(3))

Description for Non-persistence | Non-persistent Connectivity (SI-14(3))
Establish connections to the system on demand and terminate connections after [Selection: completion of a request; a period of non-use].

Discussion for Non-persistence | Non-persistent Connectivity (SI-14(3))
Persistent connections to systems can provide advanced adversaries with paths to move laterally through systems and potentially position themselves closer to high value assets. Limiting the availability of such connections impedes the adversary's ability to move freely through organizational systems.

Information Output Filtering (SI-15)

Description for Information Output Filtering (SI-15)
Validate information output 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].

Discussion for Information Output Filtering (SI-15)
Certain types of attacks, including SQL injections, produce output results that are unexpected or inconsistent with the output results that would be expected from software programs or applications. Information output filtering focuses on detecting extraneous content, preventing such extraneous content from being displayed, and then alerting monitoring tools that anomalous behavior has been discovered.

Memory Protection (SI-16)

Description for Memory Protection (SI-16)
Implement the following controls to protect the system memory from unauthorized code execution: [Assignment: organization-defined controls].

Discussion for Memory Protection (SI-16)
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 either be hardware-enforced or software-enforced with hardware enforcement providing the greater strength of mechanism.

Fail-safe Procedures (SI-17)

Description for Fail-safe Procedures (SI-17)
Implement the indicated fail-safe procedures when the indicated failures occur: [Assignment: organization-defined list of failure conditions and associated fail-safe procedures].

Discussion for Fail-safe Procedures (SI-17)
Failure conditions include the 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. Subsequent steps may include doing nothing, reestablishing system settings, shutting down processes, restarting the system, or contacting designated organizational personnel.

Personally Identifiable Information Quality Operations (SI-18)

Description for Personally Identifiable Information Quality Operations (SI-18)
a. Check the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle [Assignment: organization-defined frequency]; and
b. Correct or delete inaccurate or outdated personally identifiable information.

Discussion for Personally Identifiable Information Quality Operations (SI-18)
Personally identifiable information quality operations include the 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 disposal of personally identifiable information. Personally identifiable information quality operations include editing and validating addresses as they are collected or entered into systems using automated address verification look-up application programming interfaces. Checking personally identifiable information quality includes the tracking of updates or changes to data over time, which enables organizations to know how and what personally identifiable information was changed should erroneous information be identified. The measures taken to protect personally identifiable information quality are based on the nature and context of the personally identifiable information, how it is to be used, how it was obtained, and the potential de-identification methods employed. The measures taken to validate the accuracy of personally identifiable information used to make determinations about the rights, benefits, or privileges of individuals covered under federal programs may be more comprehensive than the measures used to validate personally identifiable information used for less sensitive purposes.

Personally Identifiable Information Quality Operations | Automation Support (SI-18(1))

Description for Personally Identifiable Information Quality Operations | Automation Support (SI-18(1))
Correct or delete personally identifiable information that is inaccurate or outdated, incorrectly determined regarding impact, or incorrectly de-identified using [Assignment: organization-defined automated mechanisms].

Discussion for Personally Identifiable Information Quality Operations | Automation Support (SI-18(1))
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 assessments and make determinations that are in alignment with their privacy program plans.
As data is obtained and used across the information life cycle, it is important to confirm 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 large-scale systems. For example, automated tools can greatly improve efforts to consistently normalize data or identify malformed data. Automated tools can also be used to improve the auditing of data and detect errors that may incorrectly alter personally identifiable information or incorrectly associate such information with the wrong individual. Automated capabilities backstop processes and procedures at-scale and enable more fine-grained detection and correction of data quality errors.

Personally Identifiable Information Quality Operations | Data Tags (SI-18(2))

Description for Personally Identifiable Information Quality Operations | Data Tags (SI-18(2))
Employ data tags to automate the correction or deletion of personally identifiable information across the information life cycle within organizational systems.

Discussion for Personally Identifiable Information Quality Operations | Data Tags (SI-18(2))
Data tagging personally identifiable information includes tags that note 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 automation tools to correct or delete relevant personally identifiable information.

Personally Identifiable Information Quality Operations | Collection (SI-18(3))

Description for Personally Identifiable Information Quality Operations | Collection (SI-18(3))
Collect personally identifiable information directly from the individual.

Discussion for Personally Identifiable Information Quality Operations | Collection (SI-18(3))
Individuals or their designated representatives can be sources of correct personally identifiable information. Organizations consider contextual factors that may incentivize individuals to provide correct data versus 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. The 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 the measures taken to validate less sensitive personally identifiable information.

Personally Identifiable Information Quality Operations | Individual Requests (SI-18(4))

Description for Personally Identifiable Information Quality Operations | Individual Requests (SI-18(4))
Correct or delete personally identifiable information upon request by individuals or their designated representatives.

Discussion for Personally Identifiable Information Quality Operations | Individual Requests (SI-18(4))
Inaccurate personally identifiable information 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 benefits of an organization maintaining the information. Organizations use discretion when determining if personally identifiable information is to be corrected or deleted based on the scope of requests, the changes sought, the impact of the changes, and laws, regulations, and policies. Organizational personnel consult with the senior agency official for privacy and legal counsel regarding appropriate instances of correction or deletion.

Personally Identifiable Information Quality Operations | Notice of Correction or Deletion (SI-18(5))

Description for Personally Identifiable Information Quality Operations | Notice of Correction or Deletion (SI-18(5))
Notify [Assignment: organization-defined recipients of personally identifiable information] and individuals that the personally identifiable information has been corrected or deleted.

Discussion for Personally Identifiable Information Quality Operations | Notice of Correction or Deletion (SI-18(5))
When personally identifiable information is corrected or deleted, organizations take steps to ensure that all authorized recipients of such information, and the individual with whom the information is associated or their designated representatives, are informed of the corrected or deleted information.

De-identification (SI-19)

Description for De-identification (SI-19)
a. 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.

Discussion for De-identification (SI-19)
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 those 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. Re-identification is a residual risk with de-identified data. Re-identification attacks can vary, including combining new datasets or other improvements in data analytics. Maintaining awareness of potential attacks and evaluating for the effectiveness of the de-identification over time support the management of this residual risk.

De-identification | Collection (SI-19(1))

Description for De-identification | Collection (SI-19(1))
De-identify the dataset upon collection by not collecting personally identifiable information.

Discussion for De-identification | Collection (SI-19(1))
If a data source contains personally identifiable information but the information will not be used, the dataset can be de-identified when it is created by not collecting the data elements that contain 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.

De-identification | Archiving (SI-19(2))

Description for De-identification | Archiving (SI-19(2))
Prohibit archiving of personally identifiable information elements if those elements in a dataset will not be needed after the dataset is archived.

Discussion for De-identification | Archiving (SI-19(2))
Datasets can be archived for many reasons. The envisioned purposes for the archived dataset are specified, and if personally identifiable information elements are not required, the elements are not archived. For example, social security numbers may have been collected for record linkage, but the archived dataset may include the required elements from the linked records. In this case, it is not necessary to archive the social security numbers.

De-identification | Release (SI-19(3))

Description for De-identification | Release (SI-19(3))
Remove personally identifiable information elements from a dataset prior to its release if those elements in the dataset do not need to be part of the data release.

Discussion for De-identification | Release (SI-19(3))
Prior to releasing a dataset, a data custodian considers the intended uses of the dataset and determines if it is necessary to release personally identifiable information. If the personally identifiable information is not necessary, the information can be removed using de-identification techniques.

De-identification | Removal, Masking, Encryption, Hashing, or Replacement of Direct Identifiers (SI-19(4))

Description for De-identification | Removal, Masking, Encryption, Hashing, or Replacement of Direct Identifiers (SI-19(4))
Remove, mask, encrypt, hash, or replace direct identifiers in a dataset.

Discussion for De-identification | Removal, Masking, Encryption, Hashing, or Replacement of Direct Identifiers (SI-19(4))
There are many possible processes for removing direct identifiers from a dataset. Columns in a dataset that contain a direct identifier can be removed. In masking, the direct identifier is transformed into a repeating character, such as XXXXXX or 999999. Identifiers can be encrypted or hashed so that the linked records remain linked. In the case of encryption or hashing, algorithms are employed that require the use of a key, including the Advanced Encryption Standard or a Hash-based Message Authentication Code. Implementations may use the same key for all identifiers or use a different key for each identifier. Using a different key for each identifier provides a higher degree of security and privacy. Identifiers can alternatively be replaced with a keyword, including transforming George Washington to PATIENT or replacing it with a surrogate value, such as transforming George Washington to Abraham Polk.

De-identification | Statistical Disclosure Control (SI-19(5))

Description for De-identification | Statistical Disclosure Control (SI-19(5))
Manipulate numerical data, contingency tables, and statistical findings so that no individual or organization is identifiable in the results of the analysis.

Discussion for De-identification | Statistical Disclosure Control (SI-19(5))
Many types of statistical analyses can result in the disclosure of information about individuals even if only summary information is provided. For example, if a school that publishes a monthly table with the number of minority students enrolled, reports that it has 10-19 such students in January, and subsequently reports that it has 20-29 such students in March, then it can be inferred that the student who enrolled in February was a minority.

De-identification | Differential Privacy (SI-19(6))

Description for De-identification | Differential Privacy (SI-19(6))
Prevent disclosure of personally identifiable information by adding non-deterministic noise to the results of mathematical operations before the results are reported.

Discussion for De-identification | Differential Privacy (SI-19(6))
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.

De-identification | Validated Algorithms and Software (SI-19(7))

Description for De-identification | Validated Algorithms and Software (SI-19(7))
Perform de-identification using validated algorithms and software that is validated to implement the algorithms.

Discussion for De-identification | Validated Algorithms and Software (SI-19(7))
Algorithms that appear to remove personally identifiable information from a dataset may in fact leave information that is personally identifiable or data that is re-identifiable. Software that is claimed to implement a validated algorithm may contain bugs or implement a different algorithm. Software may de-identify one type of data, such as integers, but not de-identify another type of data, such as floating point numbers. For these reasons, de-identification is performed using algorithms and software that are validated.

De-identification | Motivated Intruder (SI-19(8))

Description for De-identification | Motivated Intruder (SI-19(8))
Perform a motivated intruder test on the de-identified dataset to determine if the identified data remains or if the de-identified data can be re-identified.

Discussion for De-identification | Motivated Intruder (SI-19(8))
A motivated intruder test is a test in which an individual or group takes a data release and specified resources and attempts to re-identify one or more individuals in the de-identified dataset. Such tests specify the amount of inside knowledge, computational resources, financial resources, data, and skills that intruders possess to conduct the tests. A motivated intruder test can determine if the 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.

Tainting (SI-20)

Description for Tainting (SI-20)
Embed data or capabilities in the following systems or system components to determine if organizational data has been exfiltrated or improperly removed from the organization: [Assignment: organization-defined systems or system components].

Discussion for Tainting (SI-20)
Many cyber-attacks target organizational information, or information that the organization holds on behalf of other entities (e.g., personally identifiable information), and exfiltrate that data. In addition, insider attacks and erroneous user procedures can remove information from the system that is in violation of the organizational policies. Tainting approaches can range from passive to active. A passive tainting approach can be as simple as adding false email names and addresses to an internal database. If the organization receives email at one of the false email addresses, it knows that the database has been compromised. Moreover, the organization knows that the email was sent by an unauthorized entity, so any packets it includes potentially contain malicious code, and that the unauthorized entity may have potentially obtained a copy of the database. Another tainting approach can include embedding false data or steganographic data in files to enable the data to be found via open-source analysis. Finally, an active tainting approach can include embedding software in the data that is able to call home, thereby alerting the organization to its capture, and possibly its location, and the path by which it was exfiltrated or removed.

Information Refresh (SI-21)

Description for Information Refresh (SI-21)
Refresh [Assignment: organization-defined information] at [Assignment: organization-defined frequencies] or generate the information on demand and delete the information when no longer needed.

Discussion for Information Refresh (SI-21)
Retaining information for longer than it is needed makes it an increasingly valuable and enticing target for adversaries. Keeping information available for the minimum period of time needed to support organizational missions or business functions reduces the opportunity for adversaries to compromise, capture, and exfiltrate that information.

Information Diversity (SI-22)

Description for Information Diversity (SI-22)
a. Identify the following alternative sources of information for [Assignment: organization-defined essential functions and services]: [Assignment: organization-defined alternative information sources]; and
b. Use an alternative information source for the execution of essential functions or services on [Assignment: organization-defined systems or system components] when the primary source of information is corrupted or unavailable.

Discussion for Information Diversity (SI-22)
Actions taken by a system service or a function are often driven by the information it receives. Corruption, fabrication, modification, or deletion of that information could impact the ability of the service function to properly carry out its intended actions. By having multiple sources of input, the service or function can continue operation if one source is corrupted or no longer available. It is possible that the alternative sources of information may be less precise or less accurate than the primary source of information. But having such sub-optimal information sources may still provide a sufficient level of quality that the essential service or function can be carried out, even in a degraded or debilitated manner.

Information Fragmentation (SI-23)

Description for Information Fragmentation (SI-23)
Based on [Assignment: organization-defined circumstances]:
a. Fragment the following information: [Assignment: organization-defined information]; and
b. Distribute the fragmented information across the following systems or system components: [Assignment: organization-defined systems or system components].

Discussion for Information Fragmentation (SI-23)
One objective of the advanced persistent threat is to exfiltrate valuable information. Once exfiltrated, there is generally no way for the organization to recover the lost information. Therefore, organizations may consider dividing the information into disparate elements and distributing those elements across multiple systems or system components and locations. Such actions will increase the adversary's work factor to capture and exfiltrate the desired information and, in so doing, increase the probability of detection. The fragmentation of information impacts the organization's ability to access the information in a timely manner. The extent of the fragmentation is dictated by the impact or classification level (and value) of the information, threat intelligence information received, and whether data tainting is used (i.e., data tainting-derived information about the exfiltration of some information could result in the fragmentation of the remaining information).

Policy and Procedures (SR-1)

Description for Policy and Procedures (SR-1)
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] supply chain risk management policy that:
(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the supply chain risk management policy and the associated supply chain risk management controls;
b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the supply chain risk management policy and procedures; and
c. Review and update the current supply chain risk management:
1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

Discussion for Policy and Procedures (SR-1)
Supply chain risk management policy and procedures address the controls in the SR family as well as supply chain-related controls in other families that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of supply chain risk management policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, 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. Events that may precipitate an update to supply chain risk management policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Supply Chain Risk Management Plan (SR-2)

Description for Supply Chain Risk Management Plan (SR-2)
a. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the following systems, system components or system services: [Assignment: organization-defined systems, system components, or system services];
b. Review and update the supply chain risk management plan [Assignment: organization-defined frequency] or as required, to address threat, organizational or environmental changes; and
c. Protect the supply chain risk management plan from unauthorized disclosure and modification.

Discussion for Supply Chain Risk Management Plan (SR-2)
The dependence on products, systems, and services from external providers, as well as the nature of the relationships with those providers, present an increasing level of risk to an organization. Threat actions that may increase security or privacy risks include unauthorized production, the insertion or use of counterfeits, tampering, theft, insertion of malicious software and hardware, and poor manufacturing and development practices in the supply chain. Supply chain risks can be endemic or systemic within a system element or component, a system, an organization, a sector, or the Nation. Managing supply chain risk is a complex, multifaceted undertaking that requires a coordinated effort across an organization to build trust relationships and communicate with internal and external stakeholders. Supply chain risk management (SCRM) activities include identifying and assessing risks, determining appropriate risk response actions, developing SCRM plans to document response actions, and monitoring performance against plans. The SCRM plan (at the system-level) is implementation specific, providing policy implementation, requirements, constraints and implications. It can either be stand-alone, or incorporated into system security and privacy plans. The SCRM plan addresses managing, implementation, and monitoring of SCRM controls and the development/sustainment of systems across the SDLC to support mission and business functions.
Because supply chains can differ significantly across and within organizations, SCRM plans are tailored to the individual program, organizational, and operational contexts. Tailored SCRM plans provide the basis for determining whether a technology, service, system component, or system is fit for purpose, and as such, the controls need to be tailored accordingly. Tailored SCRM plans help organizations focus their resources on the most critical mission and business functions based on mission and business requirements and their risk environment. Supply chain risk management plans include an expression of the supply chain risk tolerance for the organization, acceptable supply chain risk mitigation strategies or controls, a process for consistently evaluating and monitoring supply chain risk,

approaches for implementing and communicating the plan, a description of and justification for supply chain risk mitigation measures taken, and associated roles and responsibilities. Finally, supply chain risk management plans address requirements for developing trustworthy, secure, privacy-protective, and resilient system components and systems, including the application of the security design principles implemented as part of life cycle-based systems security engineering processes (see SA-8).

Supply Chain Risk Management Plan | Establish SCRM Team (SR-2(1))

Description for Supply Chain Risk Management Plan | Establish SCRM Team (SR-2(1))
Establish a supply chain risk management team consisting of [Assignment: organization-defined personnel, roles, and responsibilities] to lead and support the following SCRM activities: [Assignment: organization-defined supply chain risk management activities].

Discussion for Supply Chain Risk Management Plan | Establish SCRM Team (SR-2(1))
To implement supply chain risk management plans, organizations establish a coordinated, team-based approach to identify and assess supply chain risks and manage these risks by using programmatic and technical mitigation techniques. The team approach enables organizations to conduct an analysis of their supply chain, communicate with internal and external partners or stakeholders, and gain broad consensus regarding the appropriate resources for SCRM. The SCRM team consists of organizational personnel with diverse roles and responsibilities for leading and supporting SCRM activities, including risk executive, information technology, contracting, information security, privacy, mission or business, legal, supply chain and logistics, acquisition, business continuity, and other relevant functions. Members of the SCRM team are involved in various aspects of the SDLC and, collectively, have an awareness of and provide expertise in acquisition processes, legal practices, vulnerabilities, threats, and attack vectors, as well as an understanding of the technical aspects and dependencies of systems. The SCRM team can be an extension of the security and privacy risk management processes or be included as part of an organizational risk management team.

Supply Chain Controls and Processes (SR-3)

Description for Supply Chain Controls and Processes (SR-3)
a. 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 personnel];
b. Employ the following controls to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain-related events: [Assignment: organization-defined supply chain controls]; and
c. Document the selected and implemented supply chain processes and controls in [Selection: security and privacy plans; supply chain risk management plan; [Assignment: organization-defined document]].

Discussion for Supply Chain Controls and Processes (SR-3)
Supply chain elements include organizations, entities, or tools employed for the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and 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, techniques, and measures to maintain provenance; or other programs, processes, 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.

Supply Chain Controls and Processes | Diverse Supply Base (SR-3(1))

Description for Supply Chain Controls and Processes | Diverse Supply Base (SR-3(1))
Employ a diverse set of sources for the following system components and services: [Assignment: organization-defined system components and services].

Discussion for Supply Chain Controls and Processes | Diverse Supply Base (SR-3(1))
Diversifying the supply of systems, system components, and services can reduce the probability that adversaries will successfully identify and target the supply chain and can reduce the impact of a supply chain event or compromise. Identifying multiple suppliers for replacement components can reduce the probability that the replacement component will become unavailable. Employing a diverse set of developers or logistics service providers can reduce the impact of a natural disaster or other supply chain event. Organizations consider designing the system to include diverse materials and components.

Supply Chain Controls and Processes | Limitation of Harm (SR-3(2))

Description for Supply Chain Controls and Processes | Limitation of Harm (SR-3(2))
Employ the following controls to limit harm from potential adversaries identifying and targeting the organizational supply chain: [Assignment: organization-defined controls].

Discussion for Supply Chain Controls and Processes | Limitation of Harm (SR-3(2))
Controls that can be implemented to reduce the probability of adversaries successfully identifying and targeting the supply chain include avoiding the purchase of custom or non-standardized configurations, employing approved vendor lists with standing reputations in industry, following pre-agreed maintenance schedules and update and patch delivery mechanisms, maintaining a contingency plan in case of a supply chain event, using procurement carve-outs that provide exclusions to commitments or obligations, using diverse delivery routes, and minimizing the time between purchase decisions and delivery.

Supply Chain Controls and Processes | Sub-tier Flow Down (SR-3(3))

Description for Supply Chain Controls and Processes | Sub-tier Flow Down (SR-3(3))
Ensure that the controls included in the contracts of prime contractors are also included in the contracts of subcontractors.

Discussion for Supply Chain Controls and Processes | Sub-tier Flow Down (SR-3(3))
To manage supply chain risk effectively and holistically, it is important that organizations ensure that supply chain risk management controls are included at all tiers in the supply chain. This includes ensuring that Tier 1 (prime) contractors have implemented processes to facilitate the flow down of supply chain risk management controls to sub-tier contractors. The controls subject to flow down are identified in SR-3b.

Provenance (SR-4)

Description for Provenance (SR-4)
Document, monitor, and maintain valid provenance of the following systems, system components, and associated data: [Assignment: organization-defined systems, system components, and associated data].

Discussion for Provenance (SR-4)
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, and changes to a system or system component and associated data. It may also include personnel and processes used to interact with or make modifications to the system, component, or associated data. Organizations consider developing procedures (see SR-1) for allocating responsibilities for the creation, maintenance, and monitoring of provenance for systems and system components; transferring provenance documentation and responsibility between organizations; and preventing and monitoring for unauthorized changes to the provenance records. Organizations have methods to document, monitor, and maintain valid provenance baselines for systems, system components, and related data. These actions help track, assess, and document any 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. Provenance considerations are addressed throughout the system development life cycle and incorporated into contracts and other arrangements, as appropriate.

Provenance | Identity (SR-4(1))

Description for Provenance | Identity (SR-4(1))
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].

Discussion for Provenance | Identity (SR-4(1))
Knowing who and what is in the supply chains of organizations is critical to gaining visibility into supply chain activities. Visibility into supply chain activities is also important for monitoring and identifying high-risk events and activities. Without reasonable visibility into supply chains elements, processes, and personnel, it is very difficult for organizations to understand and manage risk and reduce their susceptibility to adverse events. Supply chain elements include organizations, entities, or tools used for the research and development, design, manufacturing, acquisition, delivery, integration, operations, 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 the research and development, design, manufacturing, acquisition, delivery, integration, operations and 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), compromise, or event.

Provenance | Track and Trace (SR-4(2))

Description for Provenance | Track and Trace (SR-4(2))
Establish and maintain unique identification of the following systems and critical system components for tracking through the supply chain: [Assignment: organization-defined systems and critical system components].

Discussion for Provenance | Track and Trace (SR-4(2))
Tracking the unique identification of systems and system components during development and transport activities provides a foundational identity structure for the establishment and maintenance of provenance. For example, system components may be labeled using serial numbers or tagged using radio-frequency identification tags. Labels and tags can help provide better visibility into the provenance of a system or system component. A system or system component may have more than one unique identifier. Identification methods are sufficient to support a forensic investigation after a supply chain compromise or event.

Provenance | Validate as Genuine and Not Altered (SR-4(3))

Description for Provenance | Validate as Genuine and Not Altered (SR-4(3))
Employ the following controls to validate that the system or system component received is genuine and has not been altered: [Assignment: organization-defined controls].

Discussion for Provenance | Validate as Genuine and Not Altered (SR-4(3))
For many systems and system components, especially hardware, there are technical means to determine if the items are genuine or have been altered, including optical and nanotechnology tagging, physically unclonable functions, side-channel analysis, cryptographic hash verifications or digital signatures, and visible anti-tamper labels or stickers. Controls can also include monitoring for out of specification performance, which can be an indicator of tampering or counterfeits. Organizations may leverage supplier and contractor processes for validating that a system or component is genuine and has not been altered and for replacing a suspect system or component. Some indications of tampering may be visible and addressable before accepting delivery, such as inconsistent packaging, broken seals, and incorrect labels. When a system or system component is suspected of being altered or counterfeit, the supplier, contractor, or original equipment manufacturer may be able to replace the item or provide a forensic capability to determine the origin of the counterfeit or altered item. Organizations can provide training to personnel on how to identify suspicious system or component deliveries.

Provenance | Supply Chain Integrity — Pedigree (SR-4(4))

Description for Provenance | Supply Chain Integrity — Pedigree (SR-4(4))
Employ [Assignment: organization-defined controls] and conduct [Assignment: organization-defined analysis] to ensure the integrity of the system and system components by validating the internal composition and provenance of critical or mission-essential technologies, products, and services.

Discussion for Provenance | Supply Chain Integrity — Pedigree (SR-4(4))
Authoritative information regarding the internal composition of system components and the provenance of technology, products, and services provides a strong basis for trust. The validation of the internal composition and provenance of technologies, products, and services is referred to as the pedigree. For microelectronics, this includes material composition of components. For software this includes the composition of open-source and proprietary code, including the version of the component at a given point in time. Pedigrees increase the assurance that the claims suppliers assert about the internal composition and provenance of the products, services, and technologies they provide are valid. The validation of the internal composition and provenance can be achieved by various evidentiary artifacts or records that manufacturers and suppliers produce during the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of technology, products, and services. Evidentiary artifacts include, but are not limited to, software identification (SWID) tags, software component inventory, the manufacturers' declarations of platform attributes (e.g., serial numbers, hardware component inventory), and measurements (e.g., firmware hashes) that are tightly bound to the hardware itself.

Acquisition Strategies, Tools, and Methods (SR-5)

Description for Acquisition Strategies, Tools, and Methods (SR-5)
Employ the following acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks: [Assignment: organization-defined acquisition strategies, contract tools, and procurement methods].

Discussion for Acquisition Strategies, Tools, and Methods (SR-5)
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 system component, using blind 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 backdoors, and poor 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 protecting development plans, documentation, and evidence are commensurate with the security and privacy requirements of the organization. Contracts may specify documentation protection requirements.

Acquisition Strategies, Tools, and Methods | Adequate Supply (SR-5(1))

Description for Acquisition Strategies, Tools, and Methods | Adequate Supply (SR-5(1))
Employ the following controls to ensure an adequate supply of [Assignment: organization-defined critical system components]: [Assignment: organization-defined controls].

Discussion for Acquisition Strategies, Tools, and Methods | Adequate Supply (SR-5(1))
Adversaries can attempt to impede organizational operations by disrupting the supply of critical system components or corrupting supplier operations. Organizations may track systems and component mean time to failure to mitigate the loss of temporary or permanent system function. Controls to ensure that adequate supplies of critical system components include the use of multiple suppliers throughout the supply chain for the identified critical components, 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.

Acquisition Strategies, Tools, and Methods | Assessments Prior to Selection, Acceptance, Modification, or Update (SR-5(2))

Description for Acquisition Strategies, Tools, and Methods | Assessments Prior to Selection, Acceptance, Modification, or Update (SR-5(2))
Assess the system, system component, or system service prior to selection, acceptance, modification, or update.

Discussion for Acquisition Strategies, Tools, and Methods | Assessments Prior to Selection, Acceptance, Modification, or Update (SR-5(2))
Organizational 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, backdoors, and counterfeits. Assessments can include evaluations; design proposal reviews; visual or physical inspection; static and dynamic analyses; visual, x-ray, or magnetic particle inspections; simulations; white, gray, or black box testing; fuzz 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 inform the supply chain risk management process. The evidence can be leveraged in follow-on assessments. Evidence and other documentation may be shared in accordance with organizational agreements.

Supplier Assessments and Reviews (SR-6)

Description for Supplier Assessments and Reviews (SR-6)
Assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide [Assignment: organization-defined frequency].

Discussion for Supplier Assessments and Reviews (SR-6)
An assessment and review of supplier risk includes security and supply chain risk management processes, foreign ownership, control or influence (FOCI), and the ability of the supplier to effectively assess subordinate second-tier and third-tier suppliers and contractors. The reviews 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 can use open-source information to monitor for indications of stolen information, poor development and quality control practices, information spillage, or counterfeits. In some cases, it may be appropriate or required to share assessment and review results with other organizations in accordance with any applicable rules, policies, or inter-organizational agreements or contracts.

Supplier Assessments and Reviews | Testing and Analysis (SR-6(1))

Description for Supplier Assessments and Reviews | Testing and Analysis (SR-6(1))
Employ [Selection (one or more): organizational analysis; independent third-party analysis; organizational testing; independent third-party testing] of the following supply chain elements, processes, and actors associated with the system, system component, or system service: [Assignment: organization-defined supply chain elements, processes, and actors].

Discussion for Supplier Assessments and Reviews | Testing and Analysis (SR-6(1))
Relationships between entities and procedures within the supply chain, including development and delivery, are considered. Supply chain elements include organizations, entities, or tools that are used for the research and development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of systems, system components, or system services. Supply chain processes include supply chain risk management programs; SCRM strategies and implementation plans; personnel and physical security programs; hardware, software, and firmware development processes; configuration management tools, techniques, and measures to maintain provenance; shipping and handling procedures; and programs, processes, or procedures associated with the production and distribution of supply chain elements. Supply chain actors are individuals with specific roles and responsibilities in the supply chain. The evidence generated and collected during analyses and testing of supply chain elements, processes, and actors is documented and used to inform organizational risk management activities and decisions.

Supply Chain Operations Security (SR-7)

Description for Supply Chain Operations Security (SR-7)
Employ the following Operations Security (OPSEC) controls to protect supply chain-related information for the system, system component, or system service: [Assignment: organization-defined Operations Security (OPSEC) controls].

Discussion for Supply Chain Operations Security (SR-7)
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 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 organizations, implementing safeguards or countermeasures to eliminate or reduce exploitable vulnerabilities and risk to an acceptable level, and considering how aggregated information may expose users or specific uses of the supply chain. Supply chain information includes user identities; uses 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 withhold mission or business information from suppliers and may include the use of intermediaries to hide the end use or users of systems, system components, or system services.

Notification Agreements (SR-8)

Description for Notification Agreements (SR-8)
Establish agreements and procedures with entities involved in the supply chain for the system, system component, or system service for the [Selection (one or more): notification of supply chain compromises; results of assessments or audits; [Assignment: organization-defined information]].

Discussion for Notification Agreements (SR-8)
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 and could be used to help the supply chain entity resolve a concern or improve its processes.

Tamper Resistance and Detection (SR-9)

Description for Tamper Resistance and Detection (SR-9)
Implement a tamper protection program for the system, system component, or system service.

Discussion for Tamper Resistance and Detection (SR-9)
Anti-tamper technologies, tools, and techniques provide a level of protection for systems, system 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.

Tamper Resistance and Detection | Multiple Stages of System Development Life Cycle (SR-9(1))

Description for Tamper Resistance and Detection | Multiple Stages of System Development Life Cycle (SR-9(1))
Employ anti-tamper technologies, tools, and techniques throughout the system development life cycle.

Discussion for Tamper Resistance and Detection | Multiple Stages of System Development Life Cycle (SR-9(1))
The system development life cycle includes research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal. Organizations use a combination of hardware and software techniques for tamper resistance and detection. Organizations use obfuscation and self-checking to make reverse engineering and modifications more difficult, time-consuming, and expensive for adversaries. The customization of systems and system components can make substitutions easier to detect and therefore limit damage.

Inspection of Systems or Components (SR-10)

Description for Inspection of Systems or Components (SR-10)
Inspect the following systems or system components [Selection (one or more): at random; at [Assignment: organization-defined frequency], upon [Assignment: organization-defined indications of need for inspection]] to detect tampering: [Assignment: organization-defined systems or system components].

Discussion for Inspection of Systems or Components (SR-10)
The inspection of systems or systems components for tamper resistance and detection addresses physical and logical tampering and is applied to systems and system components removed from organization-controlled areas. Indications of a need for inspection include changes in packaging, specifications, factory location, or entity in which the part is purchased, and when individuals return from travel to high-risk locations.

Component Authenticity (SR-11)

Description for Component Authenticity (SR-11)
a. Develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system; and
b. Report counterfeit system components to [Selection (one or more): source of counterfeit component; [Assignment: organization-defined external reporting organizations]; [Assignment: organization-defined personnel or roles]].

Discussion for Component Authenticity (SR-11)
Sources of counterfeit components include manufacturers, developers, vendors, and contractors. Anti-counterfeiting policies and procedures support tamper resistance and provide a level of protection against the introduction of malicious code. External reporting organizations include CISA.

Component Authenticity | Anti-counterfeit Training (SR-11(1))

Description for Component Authenticity | Anti-counterfeit Training (SR-11(1))
Train [Assignment: organization-defined personnel or roles] to detect counterfeit system components (including hardware, software, and firmware).

Discussion for Component Authenticity | Anti-counterfeit Training (SR-11(1))
None.

Component Authenticity | Configuration Control for Component Service and Repair (SR-11(2))

Description for Component Authenticity | Configuration Control for Component Service and Repair (SR-11(2))
Maintain configuration control over the following system components awaiting service or repair and serviced or repaired components awaiting return to service: [Assignment: organization-defined system components].

Discussion for Component Authenticity | Configuration Control for Component Service and Repair (SR-11(2))
None.

Component Authenticity | Anti-counterfeit Scanning (SR-11(3))

Description for Component Authenticity | Anti-counterfeit Scanning (SR-11(3))
Scan for counterfeit system components [Assignment: organization-defined frequency].

Discussion for Component Authenticity | Anti-counterfeit Scanning (SR-11(3))
The type of component determines the type of scanning to be conducted (e.g., web application scanning if the component is a web application).

Component Disposal (SR-12)

Description for Component Disposal (SR-12)
Dispose of [Assignment: organization-defined data, documentation, tools, or system components] using the following techniques and methods: [Assignment: organization-defined techniques and methods].

Discussion for Component Disposal (SR-12)
Data, documentation, tools, or system components can be disposed of at any time during the system development life cycle (not only in the disposal or retirement phase of the life cycle). For example, disposal can occur during research and development, design, prototyping, or operations/maintenance and include methods such as disk cleaning, removal of cryptographic keys, partial reuse of components. Opportunities for compromise during disposal affect physical and logical data, including system documentation in paper-based or digital files; shipping and delivery documentation; memory sticks with software code; or complete routers or servers that include permanent media, which contain sensitive or proprietary information. Additionally, proper disposal of system components helps to prevent such components from entering the gray market.