Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
AC-1	Policy and Procedures	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].	Access control policy and procedures address the controls in the AC family that are implemented v	IA-1, PM-9, PM-24, PS-8, SI-12 .
AC-2	Account Management	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];	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	AC-3, AC-5, AC-6, AC-17, AC-18, AC-20, AC-24, AU-2, AU-12, CM-5, IA-2, IA-4, IA-5, IA-8, MA-3, MA-5, PE-2, PL-4, PS-2, PS-4, PS-5, PS-7, PT-2, PT-3, SC-7, SC-12, SC-13, SC-37.
AC-2(1)	Account Management | Automated System Account Management	Support the management of system accounts using [Assignment: organization-defined automated mechanisms].	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.	None.
AC-2(2)	Account Management | Automated Temporary and Emergency Account Management	Automatically [Selection: remove; disable] temporary and emergency accounts after [Assignment: organization-defined time period for each type of account].	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.	None.
AC-2(3)	Account Management | Disable Accounts	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].	Disabling expired, inactive, or otherwise anomalous accounts supports the concepts of least privilege and least functionality which reduce the attack surface of the system.	None.
AC-2(4)	Account Management | Automated Audit Actions	Automatically audit account creation, modification, enabling, disabling, and removal actions.	Account management audit records are defined in accordance with AU-2 and reviewed, analyzed,	AU-2, AU-6.
AC-2(5)	Account Management | Inactivity Logout	Require that users log out when [Assignment: organization-defined time period of expected inacti	Inactivity logout is behavior- or policy-based and requires users to take physical action to log out v	AC-11.
AC-2(6)	Account Management | Dynamic Privilege Management	Implement [Assignment: organization-defined dynamic privilege management capabilities].	In contrast to access control approaches that employ static accounts and predefined user privilege	AC-16.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
AC-2(7)	Account Management | Privileged User Accounts	(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.	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.	None.
AC-2(8)	Account Management | Dynamic Account Management	Create, activate, manage, and deactivate [Assignment: organization-defined system accounts] dyn	Approaches for dynamically creating, activating, managing, and deactivating system accounts rely	AC-16.
AC-2(9)	Account Management | Restrictions on Use of Shared and Group Accounts	Only permit the use of shared and group accounts that meet [Assignment: organization-defined conditions for establishing shared and group accounts].	Before permitting the use of shared or group accounts, organizations consider the increased risk due to the lack of accountability with such accounts.	None.
AC-13	Supervision and Review — Access Control	[Withdrawn: Incorporated into AC-2 and AU-6.]		
AC-2(11)	Account Management | Usage Conditions	Enforce [Assignment: organization-defined circumstances and/or usage conditions] for [Assignment: organization-defined system accounts].	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.	None.
AC-2(12)	Account Management | Account Monitoring for Atypical Usage	(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].	Atypical usage includes accessing systems at certain times of the day or from locations that are no	AU-6, AU-7, CA-7, IR-8, SI-4.
AC-2(13)	Account Management | Disable Accounts for High-risk Individuals	Disable accounts of individuals within [Assignment: organization-defined time period] of discovery	Users who pose a significant security and/or privacy risk include individuals for whom reliable evid	AU-6, SI-4.
AC-3	Access Enforcement	Enforce approved authorizations for logical access to information and system resources in accorda	Access control policies control access between active entities or subjects (i.e., users or processes a	AC-2, AC-4, AC-5, AC-6, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AC-24, AC-25, AT-2, AT-3, AU-9, CA-9, CM-5, CM-11, IA-2, IA-5, IA-6, IA-7, IA-11, MA-3, MA-4, MA-5, MP-4, PM-2, PS-3, PT-2, PT-3, SA-17, SC-2, SC-3, SC-4, SC-12, SC-13, SC-28, SC-31, SC-34, SI-4, SI-8.
AC-14(1)	Permitted Actions Without Identification or Authentication | Necessary Uses	[Withdrawn: Incorporated into AC-14.]		
AC-3(2)	Access Enforcement | Dual Authorization	Enforce dual authorization for [Assignment: organization-defined privileged commands and/or ot	Dual authorization, also known as two-person control, reduces risk related to insider threats. Dua	CP-9, MP-6.
AC-3(3)	Access Enforcement | Mandatory Access Control	Enforce [Assignment: organization-defined mandatory access control policy] over the set of	Mandatory access control is a type of nondiscretionary access control. Mandatory access control	SC-7.
AC-3(4)	Access Enforcement | Discretionary Access Control	Enforce [Assignment: organization-defined discretionary access control policy] over the set of	When discretionary access control policies are implemented, subjects are not constrained with	None.
AC-3(5)	Access Enforcement | Security-relevant Information	Prevent access to [Assignment: organization-defined security-relevant information] except during	Security-relevant information is information within systems that can potentially impact the operat	CM-6, SC-39.
AC-15	Automated Marking	[Withdrawn: Incorporated into MP-3.]		
AC-3(7)	Access Enforcement | Role-based Access Control	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].	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.	None.
AC-3(8)	Access Enforcement | Revocation of Access Authorizations	Enforce the revocation of access authorizations resulting from changes to the security attributes of subjects and objects based on [Assignment: organization-defined rules governing the timing of revocations of access authorizations].	Revocation of access rules may differ based on the 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.	None.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
AC-3(9)	Access Enforcement | Controlled Release	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.	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.	CA-3, PT-7, PT-8, SA-9, SC-16.
AC-3(10)	Access Enforcement | Audited Override of Access Control Mechanisms	Employ an audited override of automated access control mechanisms under [Assignment: organiz	In certain situations, such as when there is a threat to human life or an event that threatens the o	AU-2, AU-6, AU-10, AU-12, AU-14.
AC-3(11)	Access Enforcement | Restrict Access to Specific Information Types	Restrict access to data repositories containing [Assignment: organization-defined information type	Restricting access to specific information is intended to provide flexibility regarding access control	CM-8, CM-12, CM-13, PM-5.
AC-3(12)	Access Enforcement | Assert and Enforce Application Access	(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.	Asserting and enforcing application access is intended to address applications that need to access	CM-7.
AC-3(13)	Access Enforcement | Attribute-based Access Control	Enforce attribute-based access control policy over defined subjects and objects and control access based upon [Assignment: organization-defined attributes to assume access permissions].	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.	None.
AC-3(14)	Access Enforcement | Individual Access	Provide [Assignment: organization-defined mechanisms] to enable individuals to have access to th	Individual access affords individuals the ability to review personally identifiable information about	IA-8, PM-22, PM-20, PM-21, PT-6.
AC-3(15)	Access Enforcement | Discretionary and Mandatory Access Control	(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.	Simultaneously implementing a mandatory access control policy and a discretionary access contro	SC-2, SC-3, AC-4.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
AC-4	Information Flow Enforcement	Enforce approved authorizations for controlling the flow of information within the system and bet	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	AC-3, AC-6, AC-16, AC-17, AC-19, AC-21, AU-10, CA-3, CA-9, CM-7, PL-9, PM-24, SA-17, SC-4, SC-7, SC-16, SC-31.
AC-4(1)	Information Flow Enforcement | Object Security and Privacy Attributes	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.	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.	None.
AC-4(2)	Information Flow Enforcement | Processing Domains	Use protected processing domains to enforce [Assignment: organization-defined information flow	Protected processing domains within systems are processing spaces that have controlled interacti	SC-39.
AC-4(3)	Information Flow Enforcement | Dynamic Information Flow Control	Enforce [Assignment: organization-defined information flow control policies].	Organizational policies regarding dynamic information flow control include allowing or disallowing	SI-4.
AC-4(4)	Information Flow Enforcement | Flow Control of Encrypted Information	Prevent encrypted information from bypassing [Assignment: organization-defined information flo	Flow control mechanisms include content checking, security policy filters, and data type identifiers	SI-4.
AC-4(5)	Information Flow Enforcement | Embedded Data Types	Enforce [Assignment: organization-defined limitations] on embedding data types within other data types.	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.	None.
AC-4(6)	Information Flow Enforcement | Metadata	Enforce information flow control based on [Assignment: organization-defined metadata].	Metadata is information that describes the characteristics of data. Metadata can include structura	AC-16, SI-7.
AC-4(7)	Information Flow Enforcement | One-way Flow Mechanisms	Enforce one-way information flows through hardware-based flow control mechanisms.	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.	None.
AC-4(8)	Information Flow Enforcement | Security and Privacy Policy Filters	(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].	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.	None.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
AC-4(9)	Information Flow Enforcement | Human Reviews	Enforce the use of human reviews for [Assignment: organization-defined information flows] under the following conditions: [Assignment: organization-defined conditions].	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.	None.
AC-4(10)	Information Flow Enforcement | Enable and Disable Security or Privacy Policy Filters	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].	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.	None.
AC-4(11)	Information Flow Enforcement | Configuration of Security or Privacy Policy Filters	Provide the capability for privileged administrators to configure [Assignment: organization-defined security or privacy policy filters] to support different security or privacy policies.	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.	None.
AC-4(12)	Information Flow Enforcement | Data Type Identifiers	When transferring information between different security domains, use [Assignment: organization-defined data type identifiers] to validate data essential for information flow decisions.	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.	None.
AC-4(13)	Information Flow Enforcement | Decomposition into Policy-relevant Subcomponents	When transferring information between different security domains, decompose information into [Assignment: organization-defined policy-relevant subcomponents] for submission to policy enforcement mechanisms.	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.	None.
AC-4(14)	Information Flow Enforcement | Security or Privacy Policy Filter Constraints	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.	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.	None.
AC-4(15)	Information Flow Enforcement | Detection of Unsanctioned Information	When transferring information between different security domains, examine the information for t	Unsanctioned information includes malicious code, information that is inappropriate for release f	SI-3.
AC-17(5)	Remote Access | Monitoring for Unauthorized Connections	[Withdrawn: Incorporated into SI-4.]		
AC-4(17)	Information Flow Enforcement | Domain Authentication	Uniquely identify and authenticate source and destination points by [Selection (one or more): org	Attribution is a critical component of a security and privacy concept of operations. The ability to id	IA-2, IA-3, IA-9.
AC-17(7)	Remote Access | Additional Protection for Security Function Access	[Withdrawn: Incorporated into AC-3(10).]		
AC-4(19)	Information Flow Enforcement | Validation of Metadata	When transferring information between different security domains, implement [Assignment: organization-defined security or privacy policy filters] on metadata.	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.	None.
AC-4(20)	Information Flow Enforcement | Approved Solutions	Employ [Assignment: organization-defined solutions in approved configurations] to control the flow of [Assignment: organization-defined information] across security domains.	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.	None.
AC-4(21)	Information Flow Enforcement | Physical or Logical Separation of Information Flows	Separate information flows logically or physically using [Assignment: organization-defined mechan	Enforcing the separation of information flows associated with defined types of data can enhance	SC-32.
AC-4(22)	Information Flow Enforcement | Access Only	Provide access from a single device to computing platforms, applications, or data residing in multiple different security domains, while preventing information flow between the different security domains.	The system provides a capability for users to access each connected security domain without providing any mechanisms to 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.	None.
AC-4(23)	Information Flow Enforcement | Modify Non-releasable Information	When transferring information between different security domains, modify non-releasable information by implementing [Assignment: organization-defined modification action].	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.	None.
AC-4(24)	Information Flow Enforcement | Internal Normalized Format	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.	Converting data into normalized forms is one of most of effective mechanisms to stop malicious attacks and large classes of data exfiltration.	None.
AC-4(25)	Information Flow Enforcement | Data Sanitization	When transferring information between different security domains, sanitize data to minimize [Sel	Data sanitization is the process of irreversibly removing or destroying data stored on a memory de	MP-6.
AC-4(26)	Information Flow Enforcement | Audit Filtering Actions	When transferring information between different security domains, record and audit content filte	Content filtering is the process of inspecting information as it traverses a cross-domain solution ar	AU-2, AU-3, AU-12.
AC-4(27)	Information Flow Enforcement | Redundant/independent Filtering Mechanisms	When transferring information between different security domains, implement content filtering solutions that provide redundant and independent filtering mechanisms for each data type.	Content filtering is the process of inspecting information as it traverses a cross-domain solution and determines if the information meets a 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.	None.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
AC-4(28)	Information Flow Enforcement | Linear Filter Pipelines	When transferring information between different security domains, implement a linear content filter pipeline that is enforced with discretionary and mandatory access controls.	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.	None.
AC-4(29)	Information Flow Enforcement | Filter Orchestration Engines	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].	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.	None.
AC-4(30)	Information Flow Enforcement | Filter Mechanisms Using Multiple Processes	When transferring information between different security domains, implement content filtering mechanisms using multiple processes.	The use of multiple processes to implement content filtering mechanisms reduces the likelihood of a single point of failure.	None.
AC-4(31)	Information Flow Enforcement | Failed Content Transfer Prevention	When transferring information between different security domains, prevent the transfer of failed content to the receiving domain.	Content that failed filtering checks can corrupt the system if transferred to the receiving domain.	None.
AC-4(32)	Information Flow Enforcement | Process Requirements for Information Transfer	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.	The processes transferring information between filter pipelines have minimum complexity and functionality to provide assurance that the processes operate correctly.	None.
AC-5	Separation of Duties	a. Identify and document [Assignment: organization-defined duties of individuals requiring separation]; and b. Define system access authorizations to support separation of duties.	Separation of duties addresses the potential for abuse of authorized privileges and helps to reduc	AC-2, AC-3, AC-6, AU-9, CM-5, CM-11, CP-9, IA-2, IA-4, IA-5, IA-12, MA-3, MA-5, PS-2, SA-8, SA-17.
AC-6	Least Privilege	Employ the principle of least privilege, allowing only authorized accesses for users (or processes a	Organizations employ least privilege for specific duties and systems. The principle of least privilege	AC-2, AC-3, AC-5, AC-16, CM-5, CM-11, PL-2, PM-12, SA-8, SA-15, SA-17, SC-38.
AC-6(1)	Least Privilege | Authorize Access to Security Functions	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].	Security functions include establishing system accounts, configuring access authorizations (i.e., pe	AC-17, AC-18, AC-19, AU-9, PE-2.
AC-6(2)	Least Privilege | Non-privileged Access for Nonsecurity Functions	Require that users of system accounts (or roles) with access to [Assignment: organization-defined	Requiring the use of non-privileged accounts when accessing nonsecurity functions limits exposur	AC-17, AC-18, AC-19, PL-4.
AC-6(3)	Least Privilege | Network Access to Privileged Commands	Authorize network access to [Assignment: organization-defined privileged commands] only for [As	Network access is any access across a network connection in lieu of local access (i.e., user being ph	AC-17, AC-18, AC-19.
AC-6(4)	Least Privilege | Separate Processing Domains	Provide separate processing domains to enable finer-grained allocation of user privileges.	Providing separate processing domains for finer-grained allocation of user privileges includes usin	AC-4, SC-2, SC-3, SC-30, SC-32, SC-39.
AC-6(5)	Least Privilege | Privileged Accounts	Restrict privileged accounts on the system to [Assignment: organization-defined personnel or role	Privileged accounts, including super user accounts, are typically described as system administrator	IA-2, MA-3, MA-4.
AC-6(6)	Least Privilege | Privileged Access by Non-organizational Users	Prohibit privileged access to the system by non-organizational users.	An organizational user is an employee or an individual considered by the organization to have the	AC-18, AC-19, IA-2, IA-8.
AC-6(7)	Least Privilege | Review of User Privileges	(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.	The need for certain assigned user privileges may change over time to reflect changes in organizat	CA-7.
AC-6(8)	Least Privilege | Privilege Levels for Code Execution	Prevent the following software from executing at higher privilege levels than users executing the software: [Assignment: organization-defined software].	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.	None.
AC-6(9)	Least Privilege | Log Use of Privileged Functions	Log the execution of privileged functions.	The misuse of privileged functions, either intentionally or unintentionally by authorized users or b	AU-2, AU-3, AU-12.
AC-6(10)	Least Privilege | Prohibit Non-privileged Users from Executing Privileged Functions	Prevent non-privileged users from executing privileged functions.	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.	None.
AC-7	Unsuccessful Logon Attempts	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.	The need to limit unsuccessful logon attempts and take subsequent action when the maximum nu	AC-2, AC-9, AU-2, AU-6, IA-5.
AC-17(8)	Remote Access | Disable Nonsecure Network Protocols	[Withdrawn: Incorporated into CM-7.]		
AC-7(2)	Unsuccessful Logon Attempts | Purge or Wipe Mobile Device	Purge or wipe information from [Assignment: organization-defined mobile devices] based on [Ass	A mobile device is a computing device that has a small form factor such that it can be carried by a	AC-19, MP-5, MP-6.
AC-7(3)	Unsuccessful Logon Attempts | Biometric Attempt Limiting	Limit the number of unsuccessful biometric logon attempts to [Assignment: organization-defined	Biometrics are probabilistic in nature. The ability to successfully authenticate can be impacted by	IA-3.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
AC-7(4)	Unsuccessful Logon Attempts | Use of Alternate Authentication Factor	(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].	The use of alternate authentication factors supports the objective of availability and allows a user	IA-3.
AC-8	System Use Notification	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.	System use notifications can be implemented using messages or warning banners displayed befor	AC-14, PL-4, SI-4.
AC-9	Previous Logon Notification	Notify the user, upon successful logon to the system, of the date and time of the last logon.	Previous logon notification is applicable to system access via human user interfaces and access to	AC-7, PL-4.
AC-9(1)	Previous Logon Notification | Unsuccessful Logons	Notify the user, upon successful logon, of the number of unsuccessful logon attempts since the last successful logon.	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.	None.
AC-9(2)	Previous Logon Notification | Successful and Unsuccessful Logons	Notify the user, upon successful logon, of the number of [Selection: successful logons; unsuccessful logon attempts; both] during [Assignment: organization-defined time period].	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.	None.
AC-9(3)	Previous Logon Notification | Notification of Account Changes	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].	Information about changes to security-related account characteristics within a specified time period allows users to recognize if changes were made without their knowledge.	None.
AC-9(4)	Previous Logon Notification | Additional Logon Information	Notify the user, upon successful logon, of the following additional information: [Assignment: organization-defined additional information].	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.	None.
AC-10	Concurrent Session Control	Limit the number of concurrent sessions for each [Assignment: organization-defined account and/	Organizations may define the maximum number of concurrent sessions for system accounts globa	SC-23.
AC-11	Device Lock	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.	Device locks are temporary actions taken to prevent logical access to organizational systems when	AC-2, AC-7, IA-11, PL-4.
AC-11(1)	Device Lock | Pattern-hiding Displays	Conceal, via the device lock, information previously visible on the display with a publicly viewable image.	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.	None.
AC-12	Session Termination	Automatically terminate a user session after [Assignment: organization-defined conditions or trigg	Session termination addresses the termination of user-initiated logical sessions (in contrast to SC-	MA-4, SC-10, SC-23.
AC-12(1)	Session Termination | User-initiated Logouts	Provide a logout capability for user-initiated communications sessions whenever authentication is used to gain access to [Assignment: organization-defined information resources].	Information resources to which users gain access via authentication include local workstations, databases, and password-protected websites or web-based services.	None.
AC-12(2)	Session Termination | Termination Message	Display an explicit logout message to users indicating the termination of authenticated communications sessions.	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.	None.
AC-12(3)	Session Termination | Timeout Warning Message	Display an explicit message to users indicating that the session will end in [Assignment: organization-defined time until end of session].	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.	None.
AC-18(2)	Wireless Access | Monitoring Unauthorized Connections	[Withdrawn: Incorporated into SI-4.]		
AC-14	Permitted Actions Without Identification or Authentication	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.	Specific user actions may be permitted without identification or authentication if organizations de	AC-8, IA-2, PL-2.
AC-19(1)	Access Control for Mobile Devices | Use of Writable and Portable Storage Devices	[Withdrawn: Incorporated into MP-7.]		
AC-19(2)	Access Control for Mobile Devices | Use of Personally Owned Portable Storage Devices	[Withdrawn: Incorporated into MP-7.]		

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
AC-16	Security and Privacy Attributes	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].	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.	AC-3, AC-4, AC-6, AC-21, AC-25, AU-2, AU-10, MP-3, PE-22, PT-2, PT-3, PT-4, SC-11, SC-16, SI-12, SI-18.
AC-16(1)	Security and Privacy Attributes | Dynamic Attribute Association	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].	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.	None.
AC-16(2)	Security and Privacy Attributes | Attribute Value Changes by Authorized Individuals	Provide authorized individuals (or processes acting on behalf of individuals) the capability to define or change the value of associated security and privacy attributes.	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.	None.
AC-16(3)	Security and Privacy Attributes | Maintenance of Attribute Associations by System	Maintain the association and integrity of [Assignment: organization-defined security and privacy attributes] to [Assignment: organization-defined subjects and objects].	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.	None.
AC-16(4)	Security and Privacy Attributes | Association of Attributes by Authorized Individuals	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).	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.	None.
AC-16(5)	Security and Privacy Attributes | Attribute Displays on Objects to Be Output	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].	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.	None.
AC-16(6)	Security and Privacy Attributes | Maintenance of Attribute Association	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].	Maintaining attribute association requires individual users (as opposed to the system) to maintain associations of defined security and privacy attributes with subjects and objects.	None.
AC-16(7)	Security and Privacy Attributes | Consistent Attribute Interpretation	Provide a consistent interpretation of security and privacy attributes transmitted between distributed system components.	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.	None.
AC-16(8)	Security and Privacy Attributes | Association Techniques and Technologies	Implement [Assignment: organization-defined techniques and technologies] in associating security	The association of security and privacy attributes to information within systems is important for	SC-12, SC-13.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
AC-16(9)	Security and Privacy Attributes | Attribute Reassignment — Regrading Mechanisms	Change security and privacy attributes associated with information only via regrading mechanisms validated using [Assignment: organization-defined techniques or procedures].	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.	None.
AC-16(10)	Security and Privacy Attributes | Attribute Configuration by Authorized Individuals	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.	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.	None.
AC-17	Remote Access	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.	Remote access is access to organizational systems (or processes acting on behalf of users) that co	AC-2, AC-3, AC-4, AC-18, AC-19, AC-20, CA-3, CM-10, IA-2, IA-3, IA-8, MA-4, PE-17, PL-2, PL-4, SC-10, SC-12, SC-13, SI-4.
AC-17(1)	Remote Access | Monitoring and Control	Employ automated mechanisms to monitor and control remote access methods.	Monitoring and control of remote access methods allows organizations to detect attacks and help	AU-2, AU-6, AU-12, AU-14.
AC-17(2)	Remote Access | Protection of Confidentiality and Integrity Using Encryption	Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access	Virtual private networks can be used to protect the confidentiality and integrity of remote access s	SC-8, SC-12, SC-13.
AC-17(3)	Remote Access | Managed Access Control Points	Route remote accesses through authorized and managed network access control points.	Organizations consider the Trusted Internet Connections (TIC) initiative DHS TIC requirements for	SC-7.
AC-17(4)	Remote Access | Privileged Commands and Access	(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.	Remote access to systems represents a significant potential vulnerability that can be exploited by	AC-6, SC-12, SC-13.
AC-19(3)	Access Control for Mobile Devices | Use of Portable Storage Devices with No Identifiable Owner	[Withdrawn: Incorporated into MP-7.]		
AC-17(6)	Remote Access | Protection of Mechanism Information	Protect information about remote access mechanisms from unauthorized use and disclosure.	Remote access to organizational information by non-organizational entities can increase the risk o	AT-2, AT-3, PS-6.
AC-2(10)	Account Management | Shared and Group Account Credential Change	[Withdrawn: Incorporated into AC-2k.]		
AC-3(1)	Access Enforcement | Restricted Access to Privileged Functions	[Withdrawn: Incorporated into AC-6.]		
AC-17(9)	Remote Access | Disconnect or Disable Access	Provide the capability to disconnect or disable remote access to the system within [Assignment: organization-defined time period].	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.	None.
AC-17(10)	Remote Access | Authenticate Remote Commands	Implement [Assignment: organization-defined mechanisms] to authenticate [Assignment: organiz	Authenticating remote commands protects against unauthorized commands and the replay of aut	SC-12, SC-13, SC-23.
AC-18	Wireless Access	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.	Wireless technologies include microwave, packet radio (ultra-high frequency or very high frequen	AC-2, AC-3, AC-17, AC-19, CA-9, CM-7, IA-2, IA-3, IA-8, PL-4, SC-40, SC-43, SI-4.
AC-18(1)	Wireless Access | Authentication and Encryption	Protect wireless access to the system using authentication of [Selection (one or more): users; devi	Wireless networking capabilities represent a significant potential vulnerability that can be exploite	SC-8, SC-12, SC-13.
AC-3(6)	Access Enforcement | Protection of User and System Information	[Withdrawn: Incorporated into MP-4 and SC-28.]		
AC-18(3)	Wireless Access | Disable Wireless Networking	Disable, when not intended for use, wireless networking capabilities embedded within system components prior to issuance and deployment.	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.	None.
AC-18(4)	Wireless Access | Restrict Configurations by Users	Identify and explicitly authorize users allowed to independently configure wireless networking cap	Organizational authorizations to allow selected users to configure wireless networking capabilities	SC-7, SC-15.
AC-18(5)	Wireless Access | Antennas and Transmission Power Levels	Select radio antennas and calibrate transmission power levels to reduce the probability that signal	Actions that may be taken to limit unauthorized use of wireless communications outside of organi	PE-19.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
AC-19	Access Control for Mobile Devices	a. Establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas; and b. Authorize the connection of mobile devices to organizational systems.	A mobile device is a computing device that has a small form factor such that it can easily be carried 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.	AC-3, AC-4, AC-7, AC-11, AC-17, AC-18, AC-20, CA-9, CM-2, CM-6, IA-2, IA-3, MP-2, MP-4, MP-5, MP-7, PL-4, SC-7, SC-34, SC-43, SI-3, SI-4.
AC-4(16)	Information Flow Enforcement | Information Transfers on Interconnected Systems	[Withdrawn: Incorporated into AC-4.]		
AC-4(18)	Information Flow Enforcement | Security Attribute Binding	[Withdrawn: Incorporated into AC-16.]		
AC-7(1)	Unsuccessful Logon Attempts | Automatic Account Lock	[Withdrawn: Incorporated into AC-7.]		
AC-19(4)	Access Control for Mobile Devices | Restrictions for Classified Information	(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].	None.	CM-8, IR-4.
AC-19(5)	Access Control for Mobile Devices | Full Device or Container-based Encryption	Employ [Selection: full-device encryption; container-based encryption] to protect the confidentiali	Container-based encryption provides a more fine-grained approach to data and information encr	SC-12, SC-13, SC-28.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
AC-20	Use of External Systems	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].	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	AC-2, AC-3, AC-17, AC-19, CA-3, PL-2, PL-4, SA-9, SC-7.
AC-20(1)	Use of External Systems | Limits on Authorized Use	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.	Limiting authorized use recognizes circumstances where individuals using external systems may n	CA-2.
AC-20(2)	Use of External Systems | Portable Storage Devices — Restricted Use	Restrict the use of organization-controlled portable storage devices by authorized individuals on e	Limits on the use of organization-controlled portable storage devices in external systems include r	MP-7, SC-41.
AC-20(3)	Use of External Systems | Non-organizationally Owned Systems — Restricted Use	Restrict the use of non-organizationally owned systems or system components to process, store, or transmit organizational information using [Assignment: organization-defined restrictions].	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.	None.
AC-20(4)	Use of External Systems | Network Accessible Storage Devices — Prohibited Use	Prohibit the use of [Assignment: organization-defined network accessible storage devices] in external systems.	Network-accessible storage devices in external systems include online storage devices in public, hybrid, or community cloud-based systems.	None.
AC-20(5)	Use of External Systems | Portable Storage Devices — Prohibited Use	Prohibit the use of organization-controlled portable storage devices by authorized individuals on e	Limits on the use of organization-controlled portable storage devices in external systems include a	MP-7, PL-4, PS-6, SC-41.
AC-21	Information Sharing	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.	Information sharing applies to information that may be restricted in some manner based on some	AC-3, AC-4, AC-16, PT-2, PT-7, RA-3, SC-15.
AC-21(1)	Information Sharing | Automated Decision Support	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.	Automated mechanisms are used to enforce information sharing decisions.	None.
AC-21(2)	Information Sharing | Information Search and Retrieval	Implement information search and retrieval services that enforce [Assignment: organization-defined information sharing restrictions].	Information search and retrieval services identify information system resources relevant to an information need.	None.
AC-22	Publicly Accessible Content	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.	In accordance with applicable laws, executive orders, directives, policies, regulations, standards, a	AC-3, AT-2, AT-3, AU-13.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
AC-23	Data Mining Protection	Employ [Assignment: organization-defined data mining prevention and detection techniques] for [	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.	PM-12, PT-2.
AC-24	Access Control Decisions	[Selection: Establish procedures; Implement mechanisms] to ensure [Assignment: organization-de	Access control decisions (also known as authorization decisions) occur when authorization inform	AC-2, AC-3.
AC-24(1)	Access Control Decisions | Transmit Access Authorization Information	Transmit [Assignment: organization-defined access authorization information] using [Assignment:	Authorization processes and access control decisions may occur in separate parts of systems or in	AU-10.
AC-24(2)	Access Control Decisions | No User or Process Identity	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.	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.	None.
AC-25	Reference Monitor	Implement a reference monitor for [Assignment: organization-defined access control policies] tha	A reference monitor is a set of design requirements on a reference validation mechanism that, as	AC-3, AC-16, SA-8, SA-17, SC-3, SC-11, SC-39, SI-13.
AT-1	Policy and Procedures	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].	Awareness and training policy and procedures address the controls in the AT family that are imple	PM-9, PS-8, SI-12.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
AT-2	Literacy Training and Awareness	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.	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.	AC-3, AC-17, AC-22, AT-3, AT-4, CP-3, IA-4, IR-2, IR-7, IR-9, PL-4, PM-13, PM-21, PS-7, PT-2, SA-8, SA-16.
AT-2(1)	Literacy Training and Awareness | Practical Exercises	Provide practical exercises in literacy training that simulate events and incidents.	Practical exercises include no-notice social engineering attempts to collect information, gain unaut	CA-2, CA-7, CP-4, IR-3.
AT-2(2)	Literacy Training and Awareness | Insider Threat	Provide literacy training on recognizing and reporting potential indicators of insider threat.	Potential indicators and possible precursors of insider threat can include behaviors such as inordi	PM-12.
AT-2(3)	Literacy Training and Awareness | Social Engineering and Mining	Provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining.	Social engineering is an attempt to trick an individual into revealing information or taking an action that can be used to breach, compromise, or otherwise adversely impact a system. Social engineering includes phishing, pretexting, impersonation, baiting, 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.	None.
AT-2(4)	Literacy Training and Awareness | Suspicious Communications and Anomalous System Behavior	Provide literacy training on recognizing suspicious communications and anomalous behavior in organizational systems using [Assignment: organization-defined indicators of malicious code].	A well-trained workforce provides another organizational control that can be employed as part of a defense-in-depth strategy to protect 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.	None.
AT-2(5)	Literacy Training and Awareness | Advanced Persistent Threat	Provide literacy training on the advanced persistent threat.	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.	None.
AT-2(6)	Literacy Training and Awareness | Cyber Threat Environment	(a) Provide literacy training on the cyber threat environment; and (b) Reflect current cyber threat information in system operations.	Since threats continue to change over time, threat literacy training by the organization is dynamic.	RA-3.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
AT-3	Role-based Training	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.	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.	AC-3, AC-17, AC-22, AT-2, AT-4, CP-3, IR-2, IR-4, IR-7, IR-9, PL-4, PM-13, PM-23, PS-7, PS-9, SA-3, SA-8, SA-11, SA-16, SR-5, SR-6, SR-11.
AT-3(1)	Role-based Training | Environmental Controls	Provide [Assignment: organization-defined personnel or roles] with initial and [Assignment: organ	Environmental controls include fire suppression and detection devices or systems, sprinkler syster	PE-1, PE-11, PE-13, PE-14, PE-15.
AT-3(2)	Role-based Training | Physical Security Controls	Provide [Assignment: organization-defined personnel or roles] with initial and [Assignment: organ	Physical security controls include physical access control devices, physical intrusion and detection	PE-2, PE-3, PE-4.
AT-3(3)	Role-based Training | Practical Exercises	Provide practical exercises in security and privacy training that reinforce training objectives.	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.	None.
AT-3(4)	Role-based Training | Suspicious Communications and Anomalous System Behavior	[Withdrawn: Moved to AT-2(4)].		
AT-3(5)	Role-based Training | Processing Personally Identifiable Information	Provide [Assignment: organization-defined personnel or roles] with initial and [Assignment: organ	Personally identifiable information processing and transparency controls include the organization	PT-2, PT-3, PT-5, PT-6.
AT-4	Training Records	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].	Documentation for specialized training may be maintained by individual supervisors at the discret	AT-2, AT-3, CP-3, IR-2, PM-14, SI-12.
AT-5	Contacts with Security Groups and Associations	[Withdrawn: Incorporated into PM-15.]		
AT-6	Training Feedback	Provide feedback on organizational training results to the following personnel [Assignment: organization-defined frequency]: [Assignment: organization-defined personnel].	Training feedback includes awareness training results and role-based training results. Training results, especially failures of personnel in critical roles, can be 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.	None.
AU-1	Policy and Procedures	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].	Audit and accountability policy and procedures address the controls in the AU family that are impl	PM-9, PS-8, SI-12.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
AU-2	Event Logging	a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging]; b. Coordinate the event logging function with other organizational entities requiring audit-related information 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].	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	AC-2, AC-3, AC-6, AC-7, AC-8, AC-16, AC-17, AU-3, AU-4, AU-5, AU-6, AU-7, AU-11, AU-12, CM-3, CM-5, CM-6, CM-13, IA-3, MA-4, MP-4, PE-3, PM-21, PT-2, PT-7, RA-8, SA-8, SC-7, SC-18, SI-3, SI-4, SI-7, SI-10, SI-11.
AU-10(5)	Non-repudiation | Digital Signatures	[Withdrawn: Incorporated into SI-7.]		
AU-14(2)	Session Audit | Capture and Record Content	[Withdrawn: Incorporated into AU-14.]		
AU-15	Alternate Audit Logging Capability	[Withdrawn: Moved to AU-5(5).]		
AU-2(1)	Event Logging | Compilation of Audit Records from Multiple Sources	[Withdrawn: Incorporated into AU-12.]		
AU-3	Content of Audit Records	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.	Audit record content that may be necessary to support the auditing function includes event descri	AU-2, AU-8, AU-12, AU-14, MA-4, PL-9, SA-8, SI-7, SI-11.
AU-3(1)	Content of Audit Records | Additional Audit Information	Generate audit records containing the following additional information: [Assignment: organization-defined additional information].	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.	None.
AU-2(2)	Event Logging | Selection of Audit Events by Component	[Withdrawn: Incorporated into AU-12.]		
AU-3(3)	Content of Audit Records | Limit Personally Identifiable Information Elements	Limit personally identifiable information contained in audit records to the following elements iden	Limiting personally identifiable information in audit records when such information is not needed	RA-3.
AU-4	Audit Log Storage Capacity	Allocate audit log storage capacity to accommodate [Assignment: organization-defined audit log re	Organizations consider the types of audit logging to be performed and the audit log processing rec	AU-2, AU-5, AU-6, AU-7, AU-9, AU-11, AU-12, AU-14, SI-4.
AU-4(1)	Audit Log Storage Capacity | Transfer to Alternate Storage	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.	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.	None.
AU-5	Response to Audit Logging Process Failures	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].	Audit logging process failures include software and hardware errors, failures in audit log capturing	AU-2, AU-4, AU-7, AU-9, AU-11, AU-12, AU-14, SI-4, SI-12.
AU-5(1)	Response to Audit Logging Process Failures | Storage Capacity Warning	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.	Organizations may have multiple audit log storage repositories distributed across multiple system components with each repository having different storage volume capacities.	None.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
AU-5(2)	Response to Audit Logging Process Failures | Real-time Alerts	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].	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).	None.
AU-5(3)	Response to Audit Logging Process Failures | Configurable Traffic Volume Thresholds	Enforce configurable network communications traffic volume thresholds reflecting limits on audit log storage capacity and [Selection: reject; delay] network traffic above those thresholds.	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.	None.
AU-5(4)	Response to Audit Logging Process Failures | Shutdown on Failure	Invoke a [Selection: full system shutdown; partial system shutdown; degraded operational mode v	Organizations determine the types of audit logging failures that can trigger automatic system shut	AU-15.
AU-5(5)	Response to Audit Logging Process Failures | Alternate Audit Logging Capability	Provide an alternate audit logging capability in the event of a failure in primary audit logging capab	Since an alternate audit logging capability may be a short-term protection solution employed until	AU-9.
AU-6	Audit Record Review, Analysis, and Reporting	a. Review and analyze system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity] 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.	Audit record review, analysis, and reporting covers information security- and privacy-related loggi	AC-2, AC-3, AC-5, AC-6, AC-7, AC-17, AU-7, AU-16, CA-2, CA-7, CM-2, CM-5, CM-6, CM-10, CM-11, IA-2, IA-3, IA-5, IA-8, IR-5, MA-4, MP-4, PE-3, PE-6, RA-5, SA-8, SC-7, SI-3, SI-4, SI-7.
AU-6(1)	Audit Record Review, Analysis, and Reporting | Automated Process Integration	Integrate audit record review, analysis, and reporting processes using [Assignment: organization-d	Organizational processes that benefit from integrated audit record review, analysis, and reporting	PM-7.
AU-2(3)	Event Logging | Reviews and Updates	[Withdrawn: Incorporated into AU-2.]		
AU-6(3)	Audit Record Review, Analysis, and Reporting | Correlate Audit Record Repositories	Analyze and correlate audit records across different repositories to gain organization-wide situati	Organization-wide situational awareness includes awareness across all three levels of risk manage	AU-12, IR-4.
AU-6(4)	Audit Record Review, Analysis, and Reporting | Central Review and Analysis	Provide and implement the capability to centrally review and analyze audit records from multiple	Automated mechanisms for centralized reviews and analyses include Security Information and Ev	AU-2, AU-12.
AU-6(5)	Audit Record Review, Analysis, and Reporting | Integrated Analysis of Audit Records	Integrate analysis of audit records with analysis of [Selection (one or more): vulnerability scanning	Integrated analysis of audit records does not require vulnerability scanning, the generation of per	AU-12, IR-4.
AU-6(6)	Audit Record Review, Analysis, and Reporting | Correlation with Physical Monitoring	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.	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.	None.
AU-6(7)	Audit Record Review, Analysis, and Reporting | Permitted Actions	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.	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.	None.
AU-6(8)	Audit Record Review, Analysis, and Reporting | Full Text Analysis of Privileged Commands	Perform a full text analysis of logged privileged commands in a physically distinct component or su	Full text analysis of privileged commands requires a distinct environment for the analysis of audit	AU-3, AU-9, AU-11, AU-12.
AU-6(9)	Audit Record Review, Analysis, and Reporting | Correlation with Information from Nontechnic	Correlate information from nontechnical sources with audit record information to enhance organi	Nontechnical sources include records that document organizational policy violations related to ha	PM-12.
AU-2(4)	Event Logging | Privileged Functions	[Withdrawn: Incorporated into AC-6(9).]		
AU-7	Audit Record Reduction and Report Generation	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.	Audit record reduction is a process that manipulates collected audit log information and organizes	AC-2, AU-2, AU-3, AU-4, AU-5, AU-6, AU-12, AU-16, CM-5, IA-5, IR-4, PM-12, SI-4.
AU-7(1)	Audit Record Reduction and Report Generation | Automatic Processing	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].	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.	None.
AU-3(2)	Content of Audit Records | Centralized Management of Planned Audit Record Content	[Withdrawn: Incorporated into PL-9.]		
AU-8	Time Stamps	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.	Time stamps generated by the system include date and time. Time is commonly expressed in Coor	AU-3, AU-12, AU-14, SC-45.
AU-6(10)	Audit Record Review, Analysis, and Reporting | Audit Level Adjustment	[Withdrawn: Incorporated into AU-6.]		
AU-6(2)	Audit Record Review, Analysis, and Reporting | Automated Security Alerts	[Withdrawn: Incorporated into SI-4.]		
AU-9	Protection of Audit Information	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.	Audit information includes all information needed to successfully audit system activity, such as au	AC-3, AC-6, AU-6, AU-11, AU-14, AU-15, MP-2, MP-4, PE-2, PE-3, PE-6, SA-8, SC-8, SI-4.
AU-9(1)	Protection of Audit Information | Hardware Write-once Media	Write audit trails to hardware-enforced, write-once media.	Writing audit trails to hardware-enforced, write-once media applies to the initial generation of au	AU-4, AU-5.
AU-9(2)	Protection of Audit Information | Store on Separate Physical Systems or Components	Store audit records [Assignment: organization-defined frequency] in a repository that is part of a p	Storing audit records in a repository separate from the audited system or system component help	AU-4, AU-5.
AU-9(3)	Protection of Audit Information | Cryptographic Protection	Implement cryptographic mechanisms to protect the integrity of audit information and audit tools	Cryptographic mechanisms used for protecting the integrity of audit information include signed ha	AU-10, SC-12, SC-13.
AU-9(4)	Protection of Audit Information | Access by Subset of Privileged Users	Authorize access to management of audit logging functionality to only [Assignment: organization-d	Individuals or roles with privileged access to a system and who are also the subject of an audit by	AC-5.
AU-9(5)	Protection of Audit Information | Dual Authorization	Enforce dual authorization for [Selection (one or more): movement; deletion] of [Assignment: org	Organizations may choose different selection options for different types of audit information. Dua	AC-3.
AU-9(6)	Protection of Audit Information | Read-only Access	Authorize read-only access to audit information to [Assignment: organization-defined subset of privileged users or roles].	Restricting privileged user or role authorizations to read-only helps to limit the potential damage to organizations that could be initiated by such users or roles, such as deleting audit records to cover up malicious activity.	None.
AU-9(7)	Protection of Audit Information | Store on Component with Different Operating System	Store audit information on a component running a different operating system than the system or	Storing auditing information on a system component running a different operating system reduce	AU-4, AU-5, AU-11, SC-29.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
AU-10	Non-repudiation	Provide irrefutable evidence that an individual (or process acting on behalf of an individual) has p	Types of individual actions covered by non-repudiation include creating information, sending and	AU-9, PM-12, SA-8, SC-8, SC-12, SC-13, SC-16, SC-17, SC-23.
AU-10(1)	Non-repudiation | Association of Identities	(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.	Binding identities to the information supports audit requirements that provide organizational pers	AC-4, AC-16.
AU-10(2)	Non-repudiation | Validate Binding of Information Producer Identity	(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.	Validating the binding of the information producer identity to the information prevents the modifi	AC-3, AC-4, AC-16.
AU-10(3)	Non-repudiation | Chain of Custody	Maintain reviewer or releaser credentials within the established chain of custody for information	Chain of custody is a process that tracks the movement of evidence through its collection, safegua	AC-4, AC-16.
AU-10(4)	Non-repudiation | Validate Binding of Information Reviewer Identity	(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.	Validating the binding of the information reviewer identity to the information at transfer or releas	AC-4, AC-16.
AU-7(2)	Audit Record Reduction and Report Generation | Automatic Sort and Search	[Withdrawn: Incorporated into AU-7(1).]		
AU-11	Audit Record Retention	Retain audit records for [Assignment: organization-defined time period consistent with records re	Organizations retain audit records until it is determined that the records are no longer needed for	AU-2, AU-4, AU-5, AU-6, AU-9, AU-14, MP-6, RA-5, SI-12.
AU-11(1)	Audit Record Retention | Long-term Retrieval Capability	Employ [Assignment: organization-defined measures] to ensure that long-term audit records generated by the system can be retrieved.	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.	None.
AU-12	Audit Record Generation	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.	Audit records can be generated from many different system components. The event types specifie	AC-6, AC-17, AU-2, AU-3, AU-4, AU-5, AU-6, AU-7, AU-14, CM-5, MA-4, MP-4, PM-12, SA-8, SC-18, SI-3, SI-4, SI-7, SI-10.
AU-12(1)	Audit Record Generation | System-wide and Time-correlated Audit Trail	Compile audit records from [Assignment: organization-defined system components] into a system	Audit trails are time-correlated if the time stamps in the individual audit records can be reliably re	AU-8, SC-45.
AU-12(2)	Audit Record Generation | Standardized Formats	Produce a system-wide (logical or physical) audit trail composed of audit records in a standardized format.	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.	None.
AU-12(3)	Audit Record Generation | Changes by Authorized Individuals	Provide and implement the capability for [Assignment: organization-defined individuals or roles] t	Permitting authorized individuals to make changes to system logging enables organizations to exte	AC-3.
AU-12(4)	Audit Record Generation | Query Parameter Audits of Personally Identifiable Information	Provide and implement the capability for auditing the parameters of user query events for data sets containing personally identifiable information.	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.	None.
AU-13	Monitoring for Information Disclosure	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].	Unauthorized disclosure of information is a form of data leakage. Open-source information includ	AC-22, PE-3, PM-12, RA-5, SC-7, SI-20.
AU-13(1)	Monitoring for Information Disclosure | Use of Automated Tools	Monitor open-source information and information sites using [Assignment: organization-defined automated mechanisms].	Automated mechanisms include commercial services that provide notifications and alerts to organizations and automated scripts to monitor new posts on websites.	None.
AU-13(2)	Monitoring for Information Disclosure | Review of Monitored Sites	Review the list of open-source information sites being monitored [Assignment: organization-defined frequency].	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.	None.
AU-13(3)	Monitoring for Information Disclosure | Unauthorized Replication of Information	Employ discovery techniques, processes, and tools to determine if external entities are replicating organizational information in an unauthorized manner.	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.	None.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
AU-14	Session Audit	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.	Session audits can include monitoring keystrokes, tracking websites visited, and recording informa	AC-3, AC-8, AU-2, AU-3, AU-4, AU-5, AU-8, AU-9, AU-11, AU-12.
AU-14(1)	Session Audit | System Start-up	Initiate session audits automatically at system start-up.	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.	None.
AU-8(1)	Time Stamps | Synchronization with Authoritative Time Source	[Withdrawn: Moved to SC-45(1).]		
AU-14(3)	Session Audit | Remote Viewing and Listening	Provide and implement the capability for authorized users to remotely view and hear content rela	None.	AC-17.
AU-8(2)	Time Stamps | Secondary Authoritative Time Source	[Withdrawn: Moved to SC-45(2).]		
AU-16	Cross-organizational Audit Logging	Employ [Assignment: organization-defined methods] for coordinating [Assignment: organization-d	When organizations use systems or services of external organizations, the audit logging capability	AU-3, AU-6, AU-7, CA-3, PT-7.
AU-16(1)	Cross-organizational Audit Logging | Identity Preservation	Preserve the identity of individuals in cross-organizational audit trails.	Identity preservation is applied when there is a need to be able to trace actions that are performe	IA-2, IA-4, IA-5, IA-8.
AU-16(2)	Cross-organizational Audit Logging | Sharing of Audit Information	Provide cross-organizational audit information to [Assignment: organization-defined organizations	Due to the distributed nature of the audit information, cross-organization sharing of audit informa	IR-4, SI-4.
AU-16(3)	Cross-organizational Audit Logging | Disassociability	Implement [Assignment: organization-defined measures] to disassociate individuals from audit information transmitted across organizational boundaries.	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.	None.
CA-1	Policy and Procedures	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].	Assessment, authorization, and monitoring policy and procedures address the controls in the CA f	PM-9, PS-8, SI-12.
CA-2	Control Assessments	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].	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	AC-20, CA-5, CA-6, CA-7, PM-9, RA-5, RA-10, SA-11, SC-38, SI-3, SI-12, SR-2, SR-3.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
CA-2(1)	Control Assessments | Independent Assessors	Employ independent assessors or assessment teams to conduct control assessments.	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.	None.
CA-2(2)	Control Assessments | Specialized Assessments	Include as part of control assessments, [Assignment: organization-defined frequency], [Selection:	Organizations can conduct specialized assessments, including verification and validation, system m	PE-3, SI-2.
CA-2(3)	Control Assessments | Leveraging Results from External Organizations	Leverage the results of control assessments performed by [Assignment: organization-defined exte	Organizations may rely on control assessments of organizational systems by other (external) orga	SA-4.
CA-3	Information Exchange	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].	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	AC-4, AC-20, AU-16, CA-6, IA-3, IR-4, PL-2, PT-7, RA-3, SA-9, SC-7, SI-12.
CA-3(1)	Information Exchange | Unclassified National Security System Connections	[Withdrawn: Moved to SC-7(25).]		
CA-3(2)	Information Exchange | Classified National Security System Connections	[Withdrawn: Moved to SC-7(26).]		
CA-3(3)	Information Exchange | Unclassified Non-national Security System Connections	[Withdrawn: Moved to SC-7(27).]		
CA-3(4)	Information Exchange | Connections to Public Networks	[Withdrawn: Moved to SC-7(28).]		
CA-3(5)	Information Exchange | Restrictions on External System Connections	[Withdrawn: Moved to SC-7(5).]		
CA-3(6)	Information Exchange | Transfer Authorizations	Verify that individuals or systems transferring data between interconnecting systems have the req	To prevent unauthorized individuals and systems from making information transfers to protected	AC-2, AC-3, AC-4.
CA-3(7)	Information Exchange | Transitive Information Exchanges	(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.	Transitive or downstream information exchanges are information exchanges between the system	SC-7.
CA-4	Security Certification	[Withdrawn: Incorporated into CA-2.]		

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
CA-5	Plan of Action and Milestones	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.	Plans of action and milestones are useful for any type of organization to track planned remedial a	CA-2, CA-7, PM-4, PM-9, RA-7, SI-2, SI-12.
CA-5(1)	Plan of Action and Milestones | Automation Support for Accuracy and Currency	Ensure the accuracy, currency, and availability of the plan of action and milestones for the system using [Assignment: organization-defined automated mechanisms].	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.	None.
CA-6	Authorization	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].	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.	CA-2, CA-3, CA-7, PM-9, PM-10, RA-3, SA-10, SI-12.
CA-6(1)	Authorization | Joint Authorization — Intra-organization	Employ a joint authorization process for the system that includes multiple authorizing officials fro	Assigning multiple authorizing officials from the same organization to serve as co-authorizing offic	AC-6.
CA-6(2)	Authorization | Joint Authorization — Inter-organization	Employ a joint authorization process for the system that includes multiple authorizing officials wit	Assigning multiple authorizing officials, at least one of whom comes from an external organization	AC-6.
CA-7	Continuous Monitoring	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].	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.	AC-2, AC-6, AC-17, AT-4, AU-6, AU-13, CA-2, CA-5, CA-6, CM-3, CM-4, CM-6, CM-11, IA-5, IR-5, MA-2, MA-3, MA-4, PE-3, PE-6, PE-14, PE-16, PE-20, PL-2, PM-4, PM-6, PM-9, PM-10, PM-12, PM-14, PM-23, PM-28, PM-31, PS-7, PT-7, RA-3, RA-5, RA-7, RA-10, SA-8, SA-9, SA-11, SC-5, SC-7, SC-18, SC-38, SC-43, SI-3, SI-4, SI-12, SR-6.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
CA-7(1)	Continuous Monitoring | Independent Assessment	Employ independent assessors or assessment teams to monitor the controls in the system on an ongoing basis.	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.	None.
CA-7(2)	Continuous Monitoring | Types of Assessments	[Withdrawn: Incorporated into CA-2.]		
CA-7(3)	Continuous Monitoring | Trend Analyses	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.	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.	None.
CA-7(4)	Continuous Monitoring | Risk Monitoring	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.	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.	None.
CA-7(5)	Continuous Monitoring | Consistency Analysis	Employ the following actions to validate that policies are established and implemented controls are operating in a consistent manner: [Assignment: organization-defined actions].	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.	None.
CA-7(6)	Continuous Monitoring | Automation Support for Monitoring	Ensure the accuracy, currency, and availability of monitoring results for the system using [Assignment: organization-defined automated mechanisms].	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.	None.
CA-8	Penetration Testing	Conduct penetration testing [Assignment: organization-defined frequency] on [Assignment: organ	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.	RA-5, RA-10, SA-11, SR-5, SR-6.
CA-8(1)	Penetration Testing | Independent Penetration Testing Agent or Team	Employ an independent penetration testing agent or team to perform penetration testing on the s	Independent penetration testing agents or teams are individuals or groups who conduct impartial	CA-2.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
CA-8(2)	Penetration Testing | Red Team Exercises	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].	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.	None.
CA-8(3)	Penetration Testing | Facility Penetration Testing	Employ a penetration testing process that includes [Assignment: organization-defined frequency]	Penetration testing of physical access points can provide information on critical vulnerabilities in t	CA-2, PE-3.
CA-9	Internal System Connections	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.	Internal system connections are connections between organizational systems and separate consti	AC-3, AC-4, AC-18, AC-19, CM-2, IA-3, SC-7, SI-12.
CA-9(1)	Internal System Connections | Compliance Checks	Perform security and privacy compliance checks on constituent system components prior to the es	Compliance checks include verification of the relevant baseline configuration.	CM-6.
CM-1	Policy and Procedures	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].	Configuration management policy and procedures address the controls in the CM family that are i	PM-9, PS-8, SA-8, SI-12.
CM-2	Baseline Configuration	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.	Baseline configurations for systems and system components include connectivity, operational, and	AC-19, AU-6, CA-9, CM-1, CM-3, CM-5, CM-6, CM-8, CM-9, CP-9, CP-10, CP-12, MA-2, PL-8, PM-5, SA-8, SA-10, SA-15, SC-18.
CM-11(1)	User-installed Software | Alerts for Unauthorized Installations	[Withdrawn: Incorporated into CM-8(3).]		
CM-2(2)	Baseline Configuration | Automation Support for Accuracy and Currency	Maintain the currency, completeness, accuracy, and availability of the baseline configuration of th	Automated mechanisms that help organizations maintain consistent baseline configurations for sy	CM-7, IA-3, RA-5.
CM-2(3)	Baseline Configuration | Retention of Previous Configurations	Retain [Assignment: organization-defined number] of previous versions of baseline configurations of the system to support rollback.	Retaining previous versions of baseline configurations to support rollback include hardware, software, firmware, configuration files, configuration records, and associated documentation.	None.
CM-2(1)	Baseline Configuration | Reviews and Updates	[Withdrawn: Incorporated into CM-2.]		
CM-2(4)	Baseline Configuration | Unauthorized Software	[Withdrawn: Incorporated into CM-7(4).]		
CM-2(6)	Baseline Configuration | Development and Test Environments	Maintain a baseline configuration for system development and test environments that is managed	Establishing separate baseline configurations for development, testing, and operational environm	CM-4, SC-3, SC-7.
CM-2(7)	Baseline Configuration | Configure Systems and Components for High-risk Areas	(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].	When it is known that systems or system components will be in high-risk areas external to the org	MP-4, MP-5.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
CM-3	Configuration Change Control	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]].	Configuration change control for organizational systems involves the systematic proposal, justifica	CA-7, CM-2, CM-4, CM-5, CM-6, CM-9, CM-11, IA-3, MA-2, PE-16, PT-6, RA-8, SA-8, SA-10, SC-28, SC-34, SC-37, SI-2, SI-3, SI-4, SI-7, SI-10, SR-11.
CM-3(1)	Configuration Change Control | Automated Documentation, Notification, and Prohibition of Changes	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.	None.	None.
CM-3(2)	Configuration Change Control | Testing, Validation, and Documentation of Changes	Test, validate, and document changes to the system before finalizing the implementation of the changes.	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.	None.
CM-3(3)	Configuration Change Control | Automated Change Implementation	Implement changes to the current system baseline and deploy the updated baseline across the installed base using [Assignment: organization-defined automated mechanisms].	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.	None.
CM-3(4)	Configuration Change Control | Security and Privacy Representatives	Require [Assignment: organization-defined security and privacy representatives] to be members of the [Assignment: organization-defined configuration change control element].	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.	None.
CM-3(5)	Configuration Change Control | Automated Security Response	Implement the following security responses automatically if baseline configurations are changed in an unauthorized manner: [Assignment: organization-defined security responses].	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.	None.
CM-3(6)	Configuration Change Control | Cryptography Management	Ensure that cryptographic mechanisms used to provide the following controls are under configura	The controls referenced in the control enhancement refer to security and privacy controls from th	SC-12.
CM-3(7)	Configuration Change Control | Review System Changes	Review changes to the system [Assignment: organization-defined frequency] or when [Assignmen	Indications that warrant a review of changes to the system and the specific circumstances justifyin	AU-6, AU-7, CM-3.
CM-3(8)	Configuration Change Control | Prevent or Restrict Configuration Changes	Prevent or restrict changes to the configuration of the system under the following circumstances: [Assignment: organization-defined circumstances].	System configuration changes can adversely affect critical system security and privacy functionality. Change restrictions can be enforced through automated mechanisms.	None.
CM-4	Impact Analyses	Analyze changes to the system to determine potential security and privacy impacts prior to chang	Organizational personnel with security or privacy responsibilities conduct impact analyses. Individ	CA-7, CM-3, CM-8, CM-9, MA-2, RA-3, RA-5, RA-8, SA-5, SA-8, SA-10, SI-2.
CM-4(1)	Impact Analyses | Separate Test Environments	Analyze changes to the system in a separate test environment before implementation in an opera	A separate test environment requires an environment that is physically or logically separate and d	SA-11, SC-7.
CM-4(2)	Impact Analyses | Verification of Controls	After system changes, verify that the impacted controls are implemented correctly, operating as in	Implementation in this context refers to installing changed code in the operational system that ma	SA-11, SC-3, SI-6.
CM-5	Access Restrictions for Change	Define, document, approve, and enforce physical and logical access restrictions associated with ch	Changes to the hardware, software, or firmware components of systems or the operational proce	AC-3, AC-5, AC-6, CM-9, PE-3, SC-28, SC-34, SC-37, SI-2, SI-10.
CM-5(1)	Access Restrictions for Change | Automated Access Enforcement and Audit Records	(a) Enforce access restrictions using [Assignment: organization-defined automated mechanisms]; and (b) Automatically generate audit records of the enforcement actions.	Organizations log system accesses associated with applying configuration changes to ensure that c	AU-2, AU-6, AU-7, AU-12, CM-6, CM-11, SI-12.
CM-2(5)	Baseline Configuration | Authorized Software	[Withdrawn: Incorporated into CM-7(5).]		
CM-5(2)	Access Restrictions for Change | Review System Changes	[Withdrawn: Incorporated into CM-3(7).]		
CM-5(4)	Access Restrictions for Change | Dual Authorization	Enforce dual authorization for implementing changes to [Assignment: organization-defined systen	Organizations employ dual authorization to help ensure that any changes to selected system comp	AC-2, AC-5, CM-3.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
CM-5(5)	Access Restrictions for Change | Privilege Limitation for Production and Operation	(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].	In many organizations, systems support multiple mission and business functions. Limiting privilege	AC-2.
CM-5(6)	Access Restrictions for Change | Limit Library Privileges	Limit privileges to change software resident within software libraries.	Software libraries include privileged programs.	AC-2.
CM-5(3)	Access Restrictions for Change | Signed Components	[Withdrawn: Moved to CM-14.]		
CM-6	Configuration Settings	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.	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.	AC-3, AC-19, AU-2, AU-6, CA-9, CM-2, CM-3, CM-5, CM-7, CM-11, CP-7, CP-9, CP-10, IA-3, IA-5, PL-8, PL-9, RA-5, SA-4, SA-5, SA-8, SA-9, SC-18, SC-28, SC-43, SI-2, SI-4, SI-6.
CM-6(1)	Configuration Settings | Automated Management, Application, and Verification	Manage, apply, and verify configuration settings for [Assignment: organization-defined system cor	Automated tools (e.g., hardening tools, baseline configuration tools) can improve the accuracy, co	CA-7.
CM-6(2)	Configuration Settings | Respond to Unauthorized Changes	Take the following actions in response to unauthorized changes to [Assignment: organization-defi	Responses to unauthorized changes to configuration settings include alerting designated organiza	IR-4, IR-6, SI-7.
CM-5(7)	Access Restrictions for Change | Automatic Implementation of Security Safeguards	[Withdrawn: Incorporated into SI-7.]		
CM-6(3)	Configuration Settings | Unauthorized Change Detection	[Withdrawn: Incorporated into SI-7.]		
CM-7	Least Functionality	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].	Systems provide a wide variety of functions and services. Some of the functions and services routi	AC-3, AC-4, CM-2, CM-5, CM-6, CM-11, RA-5, SA-4, SA-5, SA-8, SA-9, SA-15, SC-2, SC-3, SC-7, SC-37, SI-4.
CM-7(1)	Least Functionality | Periodic Review	(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].	Organizations review functions, ports, protocols, and services provided by systems or system com	AC-18.
CM-7(2)	Least Functionality | Prevent Program Execution	Prevent program execution in accordance with [Selection (one or more): [Assignment: organizatio	Prevention of program execution addresses organizational policies, rules of behavior, and/or acce	CM-8, PL-4, PL-9, PM-5, PS-6.
CM-7(3)	Least Functionality | Registration Compliance	Ensure compliance with [Assignment: organization-defined registration requirements for functions, ports, protocols, and services].	Organizations use the registration process to manage, track, and provide oversight for systems and implemented functions, ports, protocols, and services.	None.
CM-7(4)	Least Functionality | Unauthorized Software — Deny-by-exception	(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].	Unauthorized software programs can be limited to specific versions or from a specific source. The	CM-6, CM-8, CM-10, PL-9, PM-5.
CM-7(5)	Least Functionality | Authorized Software — Allow-by-exception	(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].	Authorized software programs can be limited to specific versions or from a specific source. To faci	CM-2, CM-6, CM-8, CM-10, PL-9, PM-5, SA-10, SC-34, SI-7.
CM-7(6)	Least Functionality | Confined Environments with Limited Privileges	Require that the following user-installed software execute in a confined physical or virtual machin	Organizations identify software that may be of concern regarding its origin or potential for contair	CM-11, SC-44.
CM-7(7)	Least Functionality | Code Execution in Protected Environments	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.	Code execution in protected environments applies to all sources of binary or machine-executable	CM-10, SC-44.
CM-7(8)	Least Functionality | Binary or Machine Executable Code	(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.	Binary or machine executable code applies to all sources of binary or machine-executable code, in	SA-5, SA-22.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
CM-7(9)	Least Functionality | Prohibiting The Use of Unauthorized Hardware	(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].	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.	None.
CM-8	System Component Inventory	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].	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.	CM-2, CM-7, CM-9, CM-10, CM-11, CM-13, CP-2, CP-9, MA-2, MA-6, PE-20, PL-9, PM-5, SA-4, SA-5, SI-2, SR-4.
CM-8(1)	System Component Inventory | Updates During Installation and Removal	Update the inventory of system components as part of component installations, removals, and sy	Organizations can improve the accuracy, completeness, and consistency of system component inv	PM-16.
CM-8(2)	System Component Inventory | Automated Maintenance	Maintain the currency, completeness, accuracy, and availability of the inventory of system components using [Assignment: organization-defined automated mechanisms].	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.	None.
CM-8(3)	System Component Inventory | Automated Unauthorized Component Detection	(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]].	Automated unauthorized component detection is applied in addition to the monitoring for unauth	AC-19, CA-7, RA-5, SC-3, SC-39, SC-44, SI-3, SI-4, SI-7.
CM-8(4)	System Component Inventory | Accountability Information	Include in the system component inventory information, a means for identifying by [Selection (on	Identifying individuals who are responsible and accountable for administering system component	AC-3.
CM-6(4)	Configuration Settings | Conformance Demonstration	[Withdrawn: Incorporated into CM-4.]		
CM-8(6)	System Component Inventory | Assessed Configurations and Approved Deviations	Include assessed component configurations and any approved deviations to current deployed configurations in the system component inventory.	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.	None.
CM-8(7)	System Component Inventory | Centralized Repository	Provide a centralized repository for the inventory of system components.	Organizations may implement centralized system component inventories that include components from all organizational systems. Centralized repositories of component inventories provide 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.	None.
CM-8(8)	System Component Inventory | Automated Location Tracking	Support the tracking of system components by geographic location using [Assignment: organization-defined automated mechanisms].	The use of automated mechanisms to track the location of system components can increase the accuracy of component inventories. Such capability may help organizations rapidly identify the location and responsible individuals of system components that have been compromised, breached, or are otherwise in need of mitigation actions. The use of tracking mechanisms can be coordinated with senior agency officials for privacy if there are implications that affect individual privacy.	None.
CM-8(9)	System Component Inventory | Assignment of Components to Systems	(a) Assign system components to a system; and (b) Receive an acknowledgement from [Assignment: organization-defined personnel or roles] of this assignment.	System components that are not assigned to a system may be unmanaged, lack the required protection, and become an organizational vulnerability.	None.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
CM-9	Configuration Management Plan	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.	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.	CM-2, CM-3, CM-4, CM-5, CM-8, PL-2, RA-8, SA-10, SI-12.
CM-9(1)	Configuration Management Plan | Assignment of Responsibility	Assign responsibility for developing the configuration management process to organizational personnel that are not directly involved in system development.	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.	None.
CM-10	Software Usage Restrictions	a. Use software and associated documentation in accordance with contract agreements and copyright laws; b. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and c. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.	Software license tracking can be accomplished by manual or automated methods, depending on o	AC-17, AU-6, CM-7, CM-8, PM-30, SC-7.
CM-10(1)	Software Usage Restrictions | Open-source Software	Establish the following restrictions on the use of open-source software: [Assignment: organization	Open-source software refers to software that is available in source code form. Certain software ri	SI-7.
CM-11	User-installed Software	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].	If provided the necessary privileges, users can install software in organizational systems. To maint	AC-3, AU-6, CM-2, CM-3, CM-5, CM-6, CM-7, CM-8, PL-4, SI-4, SI-7.
CM-8(5)	System Component Inventory | No Duplicate Accounting of Components	[Withdrawn: Incorporated into CM-8.]		
CM-11(2)	User-installed Software | Software Installation with Privileged Status	Allow user installation of software only with explicit privileged status.	Privileged status can be obtained, for example, by serving in the role of system administrator.	AC-5, AC-6.
CM-11(3)	User-installed Software | Automated Enforcement and Monitoring	Enforce and monitor compliance with software installation policies using [Assignment: organization-defined automated mechanisms].	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.	None.
CM-12	Information Location	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.	Information location addresses the need to understand where information is being processed and	AC-2, AC-3, AC-4, AC-6, AC-23, CM-8, PM-5, RA-2, SA-4, SA-8, SA-17, SC-4, SC-16, SC-28, SI-4, SI-7.
CM-12(1)	Information Location | Automated Tools to Support Information Location	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.	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.	None.
CM-13	Data Action Mapping	Develop and document a map of system data actions.	Data actions are system operations that process personally identifiable information. The processi	AC-3, CM-4, CM-12, PM-5, PM-27, PT-2, PT-3, RA-3, RA-8.
CM-14	Signed Components	Prevent the installation of [Assignment: organization-defined software and firmware components	Software and firmware components prevented from installation unless signed with recognized an	CM-7, SC-12, SC-13, SI-7.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
CP-1	Policy and Procedures	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].	Contingency planning policy and procedures address the controls in the CP family that are implem	PM-9, PS-8, SI-12.
CP-2	Contingency Plan	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.	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.	CP-3, CP-4, CP-6, CP-7, CP-8, CP-9, CP-10, CP-11, CP-13, IR-4, IR-6, IR-8, IR-9, MA-6, MP-2, MP-4, MP-5, PL-2, PM-8, PM-11, SA-15, SA-20, SC-7, SC-23, SI-12.
CP-2(1)	Contingency Plan | Coordinate with Related Plans	Coordinate contingency plan development with organizational elements responsible for related plans.	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.	None.
CP-2(2)	Contingency Plan | Capacity Planning	Conduct capacity planning so that necessary capacity for information processing, telecommunicati	Capacity planning is needed because different threats can result in a reduction of the available pr	PE-11, PE-12, PE-13, PE-14, PE-18, SC-5.
CP-2(3)	Contingency Plan | Resume Mission and Business Functions	Plan for the resumption of [Selection: all; essential] mission and business functions within [Assignment: organization-defined time period] of contingency plan activation.	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.	None.
CP-10(1)	System Recovery and Reconstitution | Contingency Plan Testing	[Withdrawn: Incorporated into CP-4.]		
CP-2(5)	Contingency Plan | Continue Mission and Business Functions	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.	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.	None.
CP-2(6)	Contingency Plan | Alternate Processing and Storage Sites	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.	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.	None.
CP-2(7)	Contingency Plan | Coordinate with External Service Providers	Coordinate the contingency plan with the contingency plans of external service providers to ensur	When the capability of an organization to carry out its mission and business functions is depender	SA-9.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
CP-2(8)	Contingency Plan | Identify Critical Assets	Identify critical system assets supporting [Selection: all; essential] mission and business functions.	Organizations may choose to identify critical assets as part of criticality analysis, business continuit	CM-8, RA-9.
CP-3	Contingency Training	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].	Contingency training provided by organizations is linked to the assigned roles and responsibilities	AT-2, AT-3, AT-4, CP-2, CP-4, CP-8, IR-2, IR-4, IR-9.
CP-3(1)	Contingency Training | Simulated Events	Incorporate simulated events into contingency training to facilitate effective response by personnel in crisis situations.	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.	None.
CP-3(2)	Contingency Training | Mechanisms Used in Training Environments	Employ mechanisms used in operations to provide a more thorough and realistic contingency training environment.	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.	None.
CP-4	Contingency Plan Testing	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.	Methods for testing contingency plans to determine the effectiveness of the plans and identify po	AT-3, CP-2, CP-3, CP-8, CP-9, IR-3, IR-4, PL-2, PM-14, SR-2.
CP-4(1)	Contingency Plan Testing | Coordinate with Related Plans	Coordinate contingency plan testing with organizational elements responsible for related plans.	Plans related to contingency planning for organizational systems include Business Continuity Plans	IR-8, PM-8.
CP-4(2)	Contingency Plan Testing | Alternate Processing Site	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.	Conditions at the alternate processing site may be significantly different than the conditions at the	CP-7.
CP-4(3)	Contingency Plan Testing | Automated Testing	Test the contingency plan using [Assignment: organization-defined automated mechanisms].	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.	None.
CP-4(4)	Contingency Plan Testing | Full Recovery and Reconstitution	Include a full recovery and reconstitution of the system to a known state as part of contingency pl	Recovery is executing contingency plan activities to restore organizational mission and business fu	CP-10, SC-24.
CP-4(5)	Contingency Plan Testing | Self-challenge	Employ [Assignment: organization-defined mechanisms] to [Assignment: organization-defined system or system component] to disrupt and adversely affect the system or system component.	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.	None.
CP-10(3)	System Recovery and Reconstitution | Compensating Security Controls	[Withdrawn: Addressed through tailoring.]		
CP-6	Alternate Storage Site	a. Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information; and b. Ensure that the alternate storage site provides controls equivalent to that of the primary site.	Alternate storage sites are geographically distinct from primary storage sites and maintain duplica	CP-2, CP-7, CP-8, CP-9, CP-10, MP-4, MP-5, PE-3, SC-36, SI-13.
CP-6(1)	Alternate Storage Site | Separation from Primary Site	Identify an alternate storage site that is sufficiently separated from the primary storage site to red	Threats that affect alternate storage sites are defined in organizational risk assessments and inclu	RA-3.
CP-6(2)	Alternate Storage Site | Recovery Time and Recovery Point Objectives	Configure the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.	Organizations establish recovery time and recovery point objectives as part of contingency planning. Configuration of the alternate storage site includes physical facilities and the systems supporting recovery operations that ensure accessibility and correct execution.	None.
CP-6(3)	Alternate Storage Site | Accessibility	Identify potential accessibility problems to the alternate storage site in the event of an area-wide d	Area-wide disruptions refer to those types of disruptions that are broad in geographic scope with	RA-3.
CP-7	Alternate Processing Site	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.	Alternate processing sites are geographically distinct from primary processing sites and provide pr	CP-2, CP-6, CP-8, CP-9, CP-10, MA-6, PE-3, PE-11, PE-12, PE-17, SC-36, SI-13.
CP-7(1)	Alternate Processing Site | Separation from Primary Site	Identify an alternate processing site that is sufficiently separated from the primary processing site	Threats that affect alternate processing sites are defined in organizational assessments of risk and	RA-3.
CP-7(2)	Alternate Processing Site | Accessibility	Identify potential accessibility problems to alternate processing sites in the event of an area-wide	Area-wide disruptions refer to those types of disruptions that are broad in geographic scope with	RA-3.
CP-7(3)	Alternate Processing Site | Priority of Service	Develop alternate processing site agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives).	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.	None.
CP-7(4)	Alternate Processing Site | Preparation for Use	Prepare the alternate processing site so that the site can serve as the operational site supporting e	Site preparation includes establishing configuration settings for systems at the alternate processin	CM-2, CM-6, CP-4.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
CP-10(5)	System Recovery and Reconstitution | Failover Capability	[Withdrawn: Incorporated into SI-13.]		
CP-7(6)	Alternate Processing Site | Inability to Return to Primary Site	Plan and prepare for circumstances that preclude returning to the primary processing site.	There may be situations that preclude an organization from returning to the primary processing site 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.	None.
CP-8	Telecommunications Services	Establish alternate telecommunications services, including necessary agreements to permit the res	Telecommunications services (for data and voice) for primary and alternate processing and storag	CP-2, CP-6, CP-7, CP-11, SC-7.
CP-8(1)	Telecommunications Services | Priority of Service Provisions	(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.	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.	None.
CP-8(2)	Telecommunications Services | Single Points of Failure	Obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.	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.	None.
CP-8(3)	Telecommunications Services | Separation of Primary and Alternate Providers	Obtain alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.	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.	None.
CP-8(4)	Telecommunications Services | Provider Contingency Plan	(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].	Reviews of provider contingency plans consider the proprietary nature of such plans. In some situ	CP-3, CP-4.
CP-8(5)	Telecommunications Services | Alternate Telecommunication Service Testing	Test alternate telecommunication services [Assignment: organization-defined frequency].	Alternate telecommunications services testing is arranged through contractual agreements with se	CP-3.
CP-9	System Backup	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.	System-level information includes system state information, operating system software, middlewa	CP-2, CP-6, CP-10, MP-4, MP-5, SC-8, SC-12, SC-13, SI-4, SI-13.
CP-9(1)	System Backup | Testing for Reliability and Integrity	Test backup information [Assignment: organization-defined frequency] to verify media reliability a	Organizations need assurance that backup information can be reliably retrieved. Reliability pertai	CP-4.
CP-9(2)	System Backup | Test Restoration Using Sampling	Use a sample of backup information in the restoration of selected system functions as part of con	Organizations need assurance that system functions can be restored correctly and can support es	CP-4.
CP-9(3)	System Backup | Separate Storage for Critical Information	Store backup copies of [Assignment: organization-defined critical system software and other secu	Separate storage for critical information applies to all critical information regardless of the type of	CM-2, CM-6, CM-8.
CP-2(4)	Contingency Plan | Resume All Mission and Business Functions	[Withdrawn: Incorporated into CP-2(3).]		
CP-9(5)	System Backup | Transfer to Alternate Storage Site	Transfer system backup information to the alternate storage site [Assignment: organization-define	System backup information can be transferred to alternate storage sites either electronically or by	CP-7, MP-3, MP-4, MP-5.
CP-9(6)	System Backup | Redundant Secondary System	Conduct system backup by maintaining a redundant secondary system that is not collocated with	The effect of system backup can be achieved by maintaining a redundant secondary system that n	CP-7.
CP-9(7)	System Backup | Dual Authorization for Deletion or Destruction	Enforce dual authorization for the deletion or destruction of [Assignment: organization-defined ba	Dual authorization ensures that deletion or destruction of backup information cannot occur unles	AC-3, AC-5, MP-2.
CP-9(8)	System Backup | Cryptographic Protection	Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of [As	The selection of cryptographic mechanisms is based on the need to protect the confidentiality and	SC-12, SC-13, SC-28.
CP-10	System Recovery and Reconstitution	Provide for the recovery and reconstitution of the system to a known state within [Assignment: or	Recovery is executing contingency plan activities to restore organizational mission and business fu	CP-2, CP-4, CP-6, CP-7, CP-9, IR-4, SA-8, SC-24, SI-13.
CP-5	Contingency Plan Update	[Withdrawn: Incorporated into CP-2.]		
CP-10(2)	System Recovery and Reconstitution | Transaction Recovery	Implement transaction recovery for systems that are transaction-based.	Transaction-based systems include database management systems and transaction processing systems. Mechanisms supporting transaction recovery include transaction rollback and transaction journaling.	None.
CP-7(5)	Alternate Processing Site | Equivalent Information Security Safeguards	Withdrawn: Incorporated into CP-7.]		
CP-10(4)	System Recovery and Reconstitution | Restore Within Time Period	Provide the capability to restore system components within [Assignment: organization-defined res	Restoration of system components includes reimaging, which restores the components to known,	CM-2, CM-6.
CP-9(4)	System Backup | Protection from Unauthorized Modification	[Withdrawn: Incorporated into CP-9.]		
CP-10(6)	System Recovery and Reconstitution | Component Protection	Protect system components used for recovery and reconstitution.	Protection of system recovery and reconstitution components (i.e., hardware, firmware, and softw	AC-3, AC-6, MP-2, MP-4, PE-3, PE-6.
CP-11	Alternate Communications Protocols	Provide the capability to employ [Assignment: organization-defined alternative communications p	Contingency plans and the contingency training or testing associated with those plans incorporate	CP-2, CP-8, CP-13.
CP-12	Safe Mode	When [Assignment: organization-defined conditions] are detected, enter a safe mode of operatio	For systems that support critical mission and business functions—including military operations, ci	CM-2, SA-8, SC-24, SI-13, SI-17.
CP-13	Alternative Security Mechanisms	Employ [Assignment: organization-defined alternative or supplemental security mechanisms] for s	Use of alternative security mechanisms supports system resiliency, contingency planning, and con	CP-2, CP-11, SI-13.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
IA-1	Policy and Procedures	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].	Identification and authentication policy and procedures address the controls in the IA family that	AC-1, PM-9, PS-8, SI-12.
IA-2	Identification and Authentication (organizational Users)	Uniquely identify and authenticate organizational users and associate that unique identification w	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.	AC-2, AC-3, AC-4, AC-14, AC-17, AC-18, AU-1, AU-6, IA-4, IA-5, IA-8, MA-4, MA-5, PE-2, PL-4, SA-4, SA-8.
IA-2(1)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Privil	Implement multi-factor authentication for access to privileged accounts.	Multi-factor authentication requires the use of two or more different factors to achieve authentica	AC-5, AC-6.
IA-2(2)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Non-	Implement multi-factor authentication for access to non-privileged accounts.	Multi-factor authentication requires the use of two or more different factors to achieve authentica	AC-5.
IA-2(11)	Identification and Authentication (organizational Users) | Remote Access — Separate Device	[Withdrawn: Incorporated into IA-2(6).]		
IA-2(3)	Identification and Authentication (organizational Users) | Local Access to Privileged Accounts	[Withdrawn: Incorporated into IA-2(1).]		
IA-2(5)	Identification and Authentication (organizational Users) | Individual Authentication with Group Authentication	When shared accounts or authenticators are employed, require users to be individually authenticated before granting access to the shared accounts or resources.	Individual authentication prior to shared group authentication mitigates the risk of using group accounts or authenticators.	None.
IA-2(6)	Identification and Authentication (organizational Users) | Access to Accounts —separate Devi	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].	The purpose of requiring a device that is separate from the system to which the user is attempting	AC-6.
IA-2(4)	Identification and Authentication (organizational Users) | Local Access to Non-privileged Accounts	[Withdrawn: Incorporated into IA-2(2).]		
IA-2(8)	Identification and Authentication (organizational Users) | Access to Accounts — Replay Resistant	Implement replay-resistant authentication mechanisms for access to [Selection (one or more): privileged accounts; non-privileged accounts].	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.	None.
IA-2(7)	Identification and Authentication (organizational Users) | Network Access to Non-privileged Accounts — Separate Device	[Withdrawn: Incorporated into IA-2(6).]		

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
IA-2(10)	Identification and Authentication (organizational Users) | Single Sign-on	Provide a single sign-on capability for [Assignment: organization-defined system accounts and services].	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.	None.
IA-2(9)	Identification and Authentication (organizational Users) | Network Access to Non-privileged Accounts — Replay Resistant	[Withdrawn: Incorporated into IA-2(8).]		
IA-2(12)	Identification and Authentication (organizational Users) | Acceptance of PIV Credentials	Accept and electronically verify Personal Identity Verification-compliant credentials.	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.	None.
IA-2(13)	Identification and Authentication (organizational Users) | Out-of-band Authentication	Implement the following out-of-band authentication mechanisms under [Assignment: organizatio	Out-of-band authentication refers to the use of two separate communication paths to identify and	IA-10, IA-11, SC-37.
IA-3	Device Identification and Authentication	Uniquely identify and authenticate [Assignment: organization-defined devices and/or types of dev	Devices that require unique device-to-device identification and authentication are defined by type	AC-17, AC-18, AC-19, AU-6, CA-3, CA-9, IA-4, IA-5, IA-9, IA-11, SI-4.
IA-3(1)	Device Identification and Authentication | Cryptographic Bidirectional Authentication	Authenticate [Assignment: organization-defined devices and/or types of devices] before establishi	A local connection is a connection with a device that communicates without the use of a network.	SC-8, SC-12, SC-13.
IA-3(2)	Device Identification and Authentication | Cryptographic Bidirectional Network Authentication	Withdrawn: Incorporated into IA-3(1).]		
IA-3(3)	Device Identification and Authentication | Dynamic Address Allocation	(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.	The Dynamic Host Configuration Protocol (DHCP) is an example of a means by which clients can dy	AU-2.
IA-3(4)	Device Identification and Authentication | Device Attestation	Handle device identification and authentication based on attestation by [Assignment: organization	Device attestation refers to the identification and authentication of a device based on its configura	CM-2, CM-3, CM-6.
IA-4	Identifier Management	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].	Common device identifiers include Media Access Control (MAC) addresses, Internet Protocol (IP) a	AC-5, IA-2, IA-3, IA-5, IA-8, IA-9, IA-12, MA-4, PE-2, PE-3, PE-4, PL-4, PM-12, PS-3, PS-4, PS-5, SC-37.
IA-4(1)	Identifier Management | Prohibit Account Identifiers as Public Identifiers	Prohibit the use of system account identifiers that are the same as public identifiers for individual	Prohibiting account identifiers as public identifiers applies to any publicly disclosed account identi	AT-2, PT-7.
IA-4(2)	Identifier Management | Supervisor Authorization	[Withdrawn: Incorporated into IA-12(1).]		
IA-4(3)	Identifier Management | Multiple Forms of Certification	[Withdrawn: Incorporated into IA-12(2).]		
IA-4(4)	Identifier Management | Identify User Status	Manage individual identifiers by uniquely identifying each individual as [Assignment: organization-defined characteristic identifying individual status].	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.	None.
IA-4(5)	Identifier Management | Dynamic Management	Manage individual identifiers dynamically in accordance with [Assignment: organization-defined d	In contrast to conventional approaches to identification that presume static accounts for preregis	AC-16.
IA-4(6)	Identifier Management | Cross-organization Management	Coordinate with the following external organizations for cross-organization management of identi	Cross-organization identifier management provides the capability to identify individuals, groups, r	AU-16, IA-2, IA-5.
IA-4(7)	Identifier Management | In-person Registration	[Withdrawn: Incorporated into IA-12(4).]		
IA-4(8)	Identifier Management | Pairwise Pseudonymous Identifiers	Generate pairwise pseudonymous identifiers.	A pairwise pseudonymous identifier is an opaque unguessable subscriber identifier generated by	IA-5.
IA-4(9)	Identifier Management | Attribute Maintenance and Protection	Maintain the attributes for each uniquely identified individual, device, or service in [Assignment: organization-defined protected central storage].	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.	None.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
IA-5	Authenticator Management	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.	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.	AC-3, AC-6, CM-6, IA-2, IA-4, IA-7, IA-8, IA-9, MA-4, PE-2, PL-4, SC-12, SC-13.
IA-5(1)	Authenticator Management | Password-based Authentication	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].	Password-based authentication applies to passwords regardless of whether they are used in singl	IA-6.
IA-5(2)	Authenticator Management | Public Key-based Authentication	(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.	Public key cryptography is a valid authentication mechanism for individuals, machines, and device	IA-3, SC-17.
IA-5(11)	Authenticator Management | Hardware Token-based Authentication	[Withdrawn: Incorporated into IA-2(1) and IA-2(2).]		
IA-5(3)	Authenticator Management | In-person or Trusted External Party Registration	[Withdrawn: Incorporated into IA-12(4).]		
IA-5(5)	Authenticator Management | Change Authenticators Prior to Delivery	Require developers and installers of system components to provide unique authenticators or change default authenticators prior to delivery and installation.	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.	None.
IA-5(6)	Authenticator Management | Protection of Authenticators	Protect authenticators commensurate with the security category of the information to which use o	For systems that contain multiple security categories of information without reliable physical or lo	RA-2.
IA-5(7)	Authenticator Management | No Embedded Unencrypted Static Authenticators	Ensure that unencrypted static authenticators are not embedded in applications or other forms of static storage.	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.	None.
IA-5(8)	Authenticator Management | Multiple System Accounts	Implement [Assignment: organization-defined security controls] to manage the risk of compromis	When individuals have accounts on multiple systems and use the same authenticators such as pas	PS-6.
IA-5(9)	Authenticator Management | Federated Credential Management	Use the following external organizations to federate credentials: [Assignment: organization-define	Federation provides organizations with the capability to authenticate individuals and devices whe	AU-7, AU-16.
IA-5(10)	Authenticator Management | Dynamic Credential Binding	Bind identities and authenticators dynamically using the following rules: [Assignment: organizatio	Authentication requires some form of binding between an identity and the authenticator that is u	AU-16, IA-5.
IA-5(4)	Authenticator Management | Automated Support for Password Strength Determination	[Withdrawn: Incorporated into IA-5(1).]		
IA-5(12)	Authenticator Management | Biometric Authentication Performance	For biometric-based authentication, employ mechanisms that satisfy the following biometric quali	Unlike password-based authentication, which provides exact matches of user-input passwords to	AC-7.
IA-5(13)	Authenticator Management | Expiration of Cached Authenticators	Prohibit the use of cached authenticators after [Assignment: organization-defined time period].	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.	None.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
IA-5(14)	Authenticator Management | Managing Content of PKI Trust Stores	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.	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.	None.
IA-5(15)	Authenticator Management | GSA-approved Products and Services	Use only General Services Administration-approved products and services for identity, credential, and access management.	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.	None.
IA-5(16)	Authenticator Management | In-person or Trusted External Party Authenticator Issuance	Require that the issuance of [Assignment: organization-defined types of and/or specific authentica	Issuing authenticators in person or by a trusted external party enhances and reinforces the trustw	IA-12.
IA-5(17)	Authenticator Management | Presentation Attack Detection for Biometric Authenticators	Employ presentation attack detection mechanisms for biometric-based authentication.	Biometric characteristics do not constitute secrets. Such characteristics can be obtained by online	AC-7.
IA-5(18)	Authenticator Management | Password Managers	(a) Employ [Assignment: organization-defined password managers] to generate and manage passwords; and (b) Protect the passwords using [Assignment: organization-defined controls].	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.	None.
IA-6	Authentication Feedback	Obscure feedback of authentication information during the authentication process to protect the	Authentication feedback from systems does not provide information that would allow unauthoriz	AC-3.
IA-7	Cryptographic Module Authentication	Implement mechanisms for authentication to a cryptographic module that meet the requirements	Authentication mechanisms may be required within a cryptographic module to authenticate an op	AC-3, IA-5, SA-4, SC-12, SC-13.
IA-8	Identification and Authentication (non-organizational Users)	Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-	Non-organizational users include system users other than organizational users explicitly covered b	AC-2, AC-6, AC-14, AC-17, AC-18, AU-6, IA-2, IA-4, IA-5, IA-10, IA-11, MA-4, RA-3, SA-4, SC-8.
IA-8(1)	Identification and Authentication (non-organizational Users) | Acceptance of PIV Credentials f	Accept and electronically verify Personal Identity Verification-compliant credentials from other fed	Acceptance of Personal Identity Verification (PIV) credentials from other federal agencies applies t	PE-3.
IA-8(2)	Identification and Authentication (non-organizational Users) | Acceptance of External Authenticators	(a) Accept only external authenticators that are NIST-compliant; and (b) Document and maintain a list of accepted external authenticators.	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.	None.
IA-8(3)	Identification and Authentication (non-organizational Users) | Use of FICAM-approved Products	[Withdrawn: Incorporated into IA-8(2).]		
IA-8(4)	Identification and Authentication (non-organizational Users) | Use of Defined Profiles	Conform to the following profiles for identity management [Assignment: organization-defined identity management profiles].	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.	None.
IA-8(5)	Identification and Authentication (non-organizational Users) | Acceptance of PVI-I Credentials	Accept and verify federated or PKI credentials that meet [Assignment: organization-defined policy].	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.	None.
IA-8(6)	Identification and Authentication (non-organizational Users) | Disassociability	Implement the following measures to disassociate user attributes or identifier assertion relationships among individuals, credential service providers, and relying parties: [Assignment: organization-defined measures].	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.	None.
IA-9	Service Identification and Authentication	Uniquely identify and authenticate [Assignment: organization-defined system services and applica	Services that may require identification and authentication include web applications using digital c	IA-3, IA-4, IA-5, SC-8.
IA-9(1)	Service Identification and Authentication | Information Exchange	[Withdrawn: Incorporated into IA-9.]		
IA-9(2)	Service Identification and Authentication | Transmission of Decisions	[Withdrawn: Incorporated into IA-9.]		
IA-10	Adaptive Authentication	Require individuals accessing the system to employ [Assignment: organization-defined supplemen	Adversaries may compromise individual authentication mechanisms employed by organizations a	IA-2, IA-8.
IA-11	Re-authentication	Require users to re-authenticate when [Assignment: organization-defined circumstances or situati	In addition to the re-authentication requirements associated with device locks, organizations may	AC-3, AC-11, IA-2, IA-3, IA-4, IA-8.
IA-12	Identity Proofing	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.	Identity proofing is the process of collecting, validating, and verifying a user's identity information	AC-5, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-8.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
IA-12(1)	Identity Proofing | Supervisor Authorization	Require that the registration process to receive an account for logical access includes supervisor or sponsor authorization.	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.	None.
IA-12(2)	Identity Proofing | Identity Evidence	Require evidence of individual identification be presented to the registration authority.	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.	None.
IA-12(3)	Identity Proofing | Identity Evidence Validation and Verification	Require that the presented identity evidence be validated and verified through [Assignment: organizational defined methods of validation and verification].	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.	None.
IA-12(4)	Identity Proofing | In-person Validation and Verification	Require that the validation and verification of identity evidence be conducted in person before a designated registration authority.	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.	None.
IA-12(5)	Identity Proofing | Address Confirmation	Require that a [Selection: registration code; notice of proofing] be delivered through an out-of-bar	To make it more difficult for adversaries to pose as legitimate users during the identity proofing pr	IA-12.
IA-12(6)	Identity Proofing | Accept Externally-proofed Identities	Accept externally-proofed identities at [Assignment: organization-defined identity assurance level]	To limit unnecessary re-proofing of identities, particularly of non-PIV users, organizations accept p	IA-3, IA-4, IA-5, IA-8.
IR-1	Policy and Procedures	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].	Incident response policy and procedures address the controls in the IR family that are implemente	PM-9, PS-8, SI-12.
IR-2	Incident Response Training	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].	Incident response training is associated with the assigned roles and responsibilities of organizatio	AT-2, AT-3, AT-4, CP-3, IR-3, IR-4, IR-8, IR-9.
IR-2(1)	Incident Response Training | Simulated Events	Incorporate simulated events into incident response training to facilitate the required response by personnel in crisis situations.	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.	None.
IR-2(2)	Incident Response Training | Automated Training Environments	Provide an incident response training environment using [Assignment: organization-defined automated mechanisms].	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.	None.
IR-2(3)	Incident Response Training | Breach	Provide incident response training on how to identify and respond to a breach, including the organization's process for reporting a breach.	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).	None.
IR-3	Incident Response Testing	Test the effectiveness of the incident response capability for the system [Assignment: organizatio	Organizations test incident response capabilities to determine their effectiveness and identify pot	CP-3, CP-4, IR-2, IR-4, IR-8, PM-14.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
IR-3(1)	Incident Response Testing | Automated Testing	Test the incident response capability using [Assignment: organization-defined automated mechanisms].	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.	None.
IR-3(2)	Incident Response Testing | Coordination with Related Plans	Coordinate incident response testing with organizational elements responsible for related plans.	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.	None.
IR-3(3)	Incident Response Testing | Continuous Improvement	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.	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.	None.
IR-4	Incident Handling	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.	Organizations recognize that incident response capabilities are dependent on the capabilities of o	AC-19, AU-6, AU-7, CM-6, CP-2, CP-3, CP-4, IR-2, IR-3, IR-5, IR-6, IR-8, PE-6, PL-2, PM-12, SA-8, SC-5, SC-7, SI-3, SI-4, SI-7.
IR-4(1)	Incident Handling | Automated Incident Handling Processes	Support the incident handling process using [Assignment: organization-defined automated mechanisms].	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.	None.
IR-4(2)	Incident Handling | Dynamic Reconfiguration	Include the following types of dynamic reconfiguration for [Assignment: organization-defined syst	Dynamic reconfiguration includes changes to router rules, access control lists, intrusion detection	AC-2, AC-4, CM-2.
IR-4(3)	Incident Handling | Continuity of Operations	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].	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).	None.
IR-4(4)	Incident Handling | Information Correlation	Correlate incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.	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.	None.
IR-4(5)	Incident Handling | Automatic Disabling of System	Implement a configurable capability to automatically disable the system if [Assignment: organization-defined security violations] are detected.	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.	None.
IR-4(6)	Incident Handling | Insider Threats	Implement an incident handling capability for incidents involving insider threats.	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.	None.
IR-4(7)	Incident Handling | Insider Threats — Intra-organization Coordination	Coordinate an incident handling capability for insider threats that includes the following organizational entities [Assignment: organization-defined entities].	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.	None.
IR-4(8)	Incident Handling | Correlation with External Organizations	Coordinate with [Assignment: organization-defined external organizations] to correlate and share	The coordination of incident information with external organizations—including mission or busine	AU-16, PM-16.
IR-4(9)	Incident Handling | Dynamic Response Capability	Employ [Assignment: organization-defined dynamic response capabilities] to respond to incidents.	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.	None.
IR-4(10)	Incident Handling | Supply Chain Coordination	Coordinate incident handling activities involving supply chain events with other organizations invo	Organizations involved in supply chain activities include product developers, system integrators, m	CA-3, MA-2, SA-9, SR-8.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
IR-4(11)	Incident Handling | Integrated Incident Response Team	Establish and maintain an integrated incident response team that can be deployed to any location	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.	AT-3.
IR-4(12)	Incident Handling | Malicious Code and Forensic Analysis	Analyze malicious code and/or other residual artifacts remaining in the system after the incident.	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.	None.
IR-4(13)	Incident Handling | Behavior Analysis	Analyze anomalous or suspected adversarial behavior in or related to [Assignment: organization-defined environments or resources].	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.	None.
IR-4(14)	Incident Handling | Security Operations Center	Establish and maintain a security operations center.	A security operations center (SOC) is the focal point for security operations and computer network defense for an organization. The purpose of the SOC is to 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.	None.
IR-4(15)	Incident Handling | Public Relations and Reputation Repair	(a) Manage public relations associated with an incident; and (b) Employ measures to repair the reputation of the organization.	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.	None.
IR-5	Incident Monitoring	Track and document incidents.	Documenting incidents includes maintaining records about each incident, the status of the inciden	AU-6, AU-7, IR-4, IR-6, IR-8, PE-6, PM-5, SC-5, SC-7, SI-3, SI-4, SI-7.
IR-5(1)	Incident Monitoring | Automated Tracking, Data Collection, and Analysis	Track incidents and collect and analyze incident information using [Assignment: organization-defined automated mechanisms].	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.	None.
IR-6	Incident Reporting	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].	The types of incidents reported, the content and timeliness of the reports, and the designated rep	CM-6, CP-2, IR-4, IR-5, IR-8, IR-9.
IR-6(1)	Incident Reporting | Automated Reporting	Report incidents using [Assignment: organization-defined automated mechanisms].	The recipients of incident reports are specified in IR-6b. Automated reporting mechanisms include	IR-7.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
IR-6(2)	Incident Reporting | Vulnerabilities Related to Incidents	Report system vulnerabilities associated with reported incidents to [Assignment: organization-defined personnel or roles].	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.	None.
IR-6(3)	Incident Reporting | Supply Chain Coordination	Provide incident information to the provider of the product or service and other organizations inv	Organizations involved in supply chain activities include product developers, system integrators, m	SR-8.
IR-7	Incident Response Assistance	Provide an incident response support resource, integral to the organizational incident response ca	Incident response support resources provided by organizations include help desks, assistance gro	AT-2, AT-3, IR-4, IR-6, IR-8, PM-22, PM-26, SA-9, SI-18.
IR-7(1)	Incident Response Assistance | Automation Support for Availability of Information and Support	Increase the availability of incident response information and support using [Assignment: organization-defined automated mechanisms].	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.	None.
IR-7(2)	Incident Response Assistance | Coordination with External Providers	(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.	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.	None.
IR-8	Incident Response Plan	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.	It is important that organizations develop and implement a coordinated approach to incident resp	AC-2, CP-2, CP-4, IR-4, IR-7, IR-9, PE-6, PL-2, SA-15, SI-12, SR-8.
IR-8(1)	Incident Response Plan | Breaches	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.	Organizations may be required by law, regulation, or policy to follow specific procedures relating t	PT-1, PT-2, PT-3, PT-4, PT-5, PT-7.
IR-9	Information Spillage Response	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].	Information spillage refers to instances where information is placed on systems that are not autho	CP-2, IR-6, PM-26, PM-27, PT-2, PT-3, PT-7, RA-7.
IR-10	Integrated Information Security Analysis Team	[Withdrawn: Moved to IR-4(11).]		
IR-9(2)	Information Spillage Response | Training	Provide information spillage response training [Assignment: organization-defined frequency].	Organizations establish requirements for responding to information spillage incidents in incident r	AT-2, AT-3, CP-3, IR-2.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
IR-9(3)	Information Spillage Response | Post-spill Operations	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].	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.	None.
IR-9(4)	Information Spillage Response | Exposure to Unauthorized Personnel	Employ the following controls for personnel exposed to information not within assigned access authorizations: [Assignment: organization-defined controls].	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.	None.
IR-9(1)	Information Spillage Response | Responsible Personnel	[Withdrawn: Incorporated into IR-9.]		
MA-1	Policy and Procedures	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].	Maintenance policy and procedures address the controls in the MA family that are implemented v	PM-9, PS-8, SI-12.
MA-2	Controlled Maintenance	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].	Controlling system maintenance addresses the information security aspects of the system mainter	CM-2, CM-3, CM-4, CM-5, CM-8, MA-4, MP-6, PE-16, SI-2, SR-3, SR-4, SR-11.
MA-2(1)	Controlled Maintenance | Record Content	[Withdrawn: Incorporated into MA-2.]		
MA-2(2)	Controlled Maintenance | Automated Maintenance Activities	(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.	The use of automated mechanisms to manage and control system maintenance programs and act	MA-3.
MA-3	Maintenance Tools	a. Approve, control, and monitor the use of system maintenance tools; and b. Review previously approved system maintenance tools [Assignment: organization-defined frequency].	Approving, controlling, monitoring, and reviewing maintenance tools address security-related issu	MA-2, PE-16.
MA-3(1)	Maintenance Tools | Inspect Tools	Inspect the maintenance tools used by maintenance personnel for improper or unauthorized mod	Maintenance tools can be directly brought into a facility by maintenance personnel or downloade	SI-7.
MA-3(2)	Maintenance Tools | Inspect Media	Check media containing diagnostic and test programs for malicious code before the media are use	If, upon inspection of media containing maintenance, diagnostic, and test programs, organizations	SI-3.
MA-3(3)	Maintenance Tools | Prevent Unauthorized Removal	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.	Organizational information includes all information owned by organizations and any information	MP-6.
MA-3(4)	Maintenance Tools | Restricted Tool Use	Restrict the use of maintenance tools to authorized personnel only.	Restricting the use of maintenance tools to only authorized personnel applies to systems that are	AC-3, AC-5, AC-6.
MA-3(5)	Maintenance Tools | Execution with Privilege	Monitor the use of maintenance tools that execute with increased privilege.	Maintenance tools that execute with increased system privilege can result in unauthorized access	AC-3, AC-6.
MA-3(6)	Maintenance Tools | Software Updates and Patches	Inspect maintenance tools to ensure the latest software updates and patches are installed.	Maintenance tools using outdated and/or unpatched software can provide a threat vector for adv	AC-3, AC-6.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
MA-4	Nonlocal Maintenance	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.	Nonlocal maintenance and diagnostic activities are conducted by individuals who communicate th	AC-2, AC-3, AC-6, AC-17, AU-2, AU-3, IA-2, IA-4, IA-5, IA-8, MA-2, MA-5, PL-2, SC-7, SC-10.
MA-4(1)	Nonlocal Maintenance | Logging and Review	(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.	Audit logging for nonlocal maintenance is enforced by AU-2. Audit events are defined in AU-2a.	AU-6, AU-12.
MA-4(2)	Nonlocal Maintenance | Document Nonlocal Maintenance	[Withdrawn: Incorporated into MA-1 and MA-4.]		
MA-4(3)	Nonlocal Maintenance | Comparable Security and Sanitization	(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.	Comparable security capability on systems, diagnostic tools, and equipment providing maintenanc	MP-6, SI-3, SI-7.
MA-4(4)	Nonlocal Maintenance | Authentication and Separation of Maintenance Sessions	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.	Communications paths can be logically separated using encryption.	None.
MA-4(5)	Nonlocal Maintenance | Approvals and Notifications	(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].	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.	None.
MA-4(6)	Nonlocal Maintenance | Cryptographic Protection	Implement the following cryptographic mechanisms to protect the integrity and confidentiality of	Failure to protect nonlocal maintenance and diagnostic communications can result in unauthorize	SC-8, SC-12, SC-13.
MA-4(7)	Nonlocal Maintenance | Disconnect Verification	Verify session and network connection termination after the completion of nonlocal maintenance	Verifying the termination of a connection once maintenance is completed ensures that connection	AC-12.
MA-5	Maintenance Personnel	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.	Maintenance personnel refers to individuals who perform hardware or software maintenance on	AC-2, AC-3, AC-5, AC-6, IA-2, IA-8, MA-4, MP-2, PE-2, PE-3, PS-7, RA-3.
MA-5(1)	Maintenance Personnel | Individuals Without Appropriate Access	(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.	Procedures for individuals who lack appropriate security clearances or who are not U.S. citizens ar	MP-6, PL-2.
MA-5(2)	Maintenance Personnel | Security Clearances for Classified Systems	Verify that personnel performing maintenance and diagnostic activities on a system processing, st	Personnel who conduct maintenance on organizational systems may be exposed to classified info	PS-3.
MA-5(3)	Maintenance Personnel | Citizenship Requirements for Classified Systems	Verify that personnel performing maintenance and diagnostic activities on a system processing, st	Personnel who conduct maintenance on organizational systems may be exposed to classified info	PS-3.
MA-5(4)	Maintenance Personnel | Foreign Nationals	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.	Personnel who conduct maintenance and diagnostic activities on organizational systems may be e	PS-3.
MA-5(5)	Maintenance Personnel | Non-system Maintenance	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.	Personnel who perform maintenance activities in other capacities not directly related to the system include physical plant personnel and custodial personnel.	None.
MA-6	Timely Maintenance	Obtain maintenance support and/or spare parts for [Assignment: organization-defined system co	Organizations specify the system components that result in increased risk to organizational operat	CM-8, CP-2, CP-7, RA-7, SA-15, SI-13, SR-2, SR-3, SR-4.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
MA-6(1)	Timely Maintenance | Preventive Maintenance	Perform preventive maintenance on [Assignment: organization-defined system components] at [Assignment: organization-defined time intervals].	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.	None.
MA-6(2)	Timely Maintenance | Predictive Maintenance	Perform predictive maintenance on [Assignment: organization-defined system components] at [Assignment: organization-defined time intervals].	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.	None.
MA-6(3)	Timely Maintenance | Automated Support for Predictive Maintenance	Transfer predictive maintenance data to a maintenance management system using [Assignment: organization-defined automated mechanisms].	A computerized maintenance management system 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.	None.
MA-7	Field Maintenance	Restrict or prohibit field maintenance on [Assignment: organization-defined systems or system co	Field maintenance is the type of maintenance conducted on a system or system component after	MA-2, MA-4, MA-5.
MP-1	Policy and Procedures	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].	Media protection policy and procedures address the controls in the MP family that are implement	PM-9, PS-8, SI-12.
MP-2	Media Access	Restrict access to [Assignment: organization-defined types of digital and/or non-digital media] to [	System media includes digital and non-digital media. Digital media includes flash drives, diskettes,	AC-19, AU-9, CP-2, CP-9, CP-10, MA-5, MP-4, MP-6, PE-2, PE-3, SC-12, SC-13, SC-34, SI-12.
MP-2(1)	Media Access | Automated Restricted Access	[Withdrawn: Incorporated into MP-4(2).]		
MP-2(2)	Media Access | Cryptographic Protection	[Withdrawn: Incorporated into SC-28(1).]		
MP-3	Media Marking	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].	Security marking refers to the application or use of human-readable security attributes. Digital me	AC-16, CP-9, MP-5, PE-22, SI-12.
MP-4	Media Storage	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.	System media includes digital and non-digital media. Digital media includes flash drives, diskettes,	AC-19, CP-2, CP-6, CP-9, CP-10, MP-2, MP-7, PE-3, PL-2, SC-12, SC-13, SC-28, SC-34, SI-12.
MP-4(1)	Media Storage | Cryptographic Protection	[Withdrawn: Incorporated into SC-28(1).]		
MP-4(2)	Media Storage | Automated Restricted Access	Restrict access to media storage areas and log access attempts and access granted using [Assignm	Automated mechanisms include keypads, biometric readers, or card readers on the external entri	AC-3, AU-2, AU-6, AU-9, AU-12, PE-3.
MP-5	Media Transport	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.	System media includes digital and non-digital media. Digital media includes flash drives, diskettes,	AC-7, AC-19, CP-2, CP-9, MP-3, MP-4, PE-16, PL-2, SC-12, SC-13, SC-28, SC-34.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
MP-5(1)	Media Transport | Protection Outside of Controlled Areas	[Withdrawn: Incorporated into MP-5.]		
MP-5(2)	Media Transport | Documentation of Activities	[Withdrawn: Incorporated into MP-5.]		
MP-5(3)	Media Transport | Custodians	Employ an identified custodian during transport of system media outside of controlled areas.	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.	None.
MP-5(4)	Media Transport | Cryptographic Protection	[Withdrawn: Incorporated into SC-28(1).]		
MP-6	Media Sanitization	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.	Media sanitization applies to all digital and non-digital system media subject to disposal or reuse,	AC-3, AC-7, AU-11, MA-2, MA-3, MA-4, MA-5, PM-22, SI-12, SI-18, SI-19, SR-11.
MP-6(1)	Media Sanitization | Review, Approve, Track, Document, and Verify	Review, approve, track, document, and verify media sanitization and disposal actions.	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.	None.
MP-6(2)	Media Sanitization | Equipment Testing	Test sanitization equipment and procedures [Assignment: organization-defined frequency] to ensure that the intended sanitization is being achieved.	Testing of sanitization equipment and procedures may be conducted by qualified and authorized external entities, including federal agencies or external service providers.	None.
MP-6(3)	Media Sanitization | Nondestructive Techniques	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].	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.	None.
MP-6(4)	Media Sanitization | Controlled Unclassified Information	[Withdrawn: Incorporated into MP-6.]		
MP-6(5)	Media Sanitization | Classified Information	[Withdrawn: Incorporated into MP-6.]		
MP-6(6)	Media Sanitization | Media Destruction	[Withdrawn: Incorporated into MP-6.]		
MP-6(7)	Media Sanitization | Dual Authorization	Enforce dual authorization for the sanitization of [Assignment: organization-defined system media	Organizations employ dual authorization to help ensure that system media sanitization cannot oc	AC-3, MP-2.
MP-6(8)	Media Sanitization | Remote Purging or Wiping of Information	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]].	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.	None.
MP-7	Media Use	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.	System media includes both digital and non-digital media. Digital media includes diskettes, magne	AC-19, AC-20, PL-4, PM-12, SC-34, SC-41.
MP-7(1)	Media Use | Prohibit Use Without Owner	[Withdrawn: Incorporated into MP-7.]		
MP-7(2)	Media Use | Prohibit Use of Sanitization-resistant Media	Prohibit the use of sanitization-resistant media in organizational systems.	Sanitization resistance refers to how resistant media are to non-destructive sanitization technique	MP-6.
MP-8	Media Downgrading	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.	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.	None.
MP-8(1)	Media Downgrading | Documentation of Process	Document system media downgrading actions.	Organizations can document the media downgrading process by providing information, such as the downgrading technique employed, the identification number of the downgraded media, and the identity of the individual that authorized and/or performed the downgrading action.	None.
MP-8(2)	Media Downgrading | Equipment Testing	Test downgrading equipment and procedures [Assignment: organization-defined frequency] to ensure that downgrading actions are being achieved.	None.	None.
MP-8(3)	Media Downgrading | Controlled Unclassified Information	Downgrade system media containing controlled unclassified information prior to public release.	The downgrading of controlled unclassified information uses approved sanitization tools, techniques, and procedures.	None.
MP-8(4)	Media Downgrading | Classified Information	Downgrade system media containing classified information prior to release to individuals without required access authorizations.	Downgrading of classified information uses approved sanitization tools, techniques, and procedures to transfer information confirmed to be unclassified from classified systems to unclassified media.	None.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
PE-1	Policy and Procedures	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].	Physical and environmental protection policy and procedures address the controls in the PE family	AT-3, PM-9, PS-8, SI-12.
PE-2	Physical Access Authorizations	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.	Physical access authorizations apply to employees and visitors. Individuals with permanent physic	AT-3, AU-9, IA-4, MA-5, MP-2, PE-3, PE-4, PE-5, PE-8, PM-12, PS-3, PS-4, PS-5, PS-6.
PE-2(1)	Physical Access Authorizations | Access by Position or Role	Authorize physical access to the facility where the system resides based on position or role.	Role-based facility access includes access by authorized permanent and regular/routine maintena	AC-2, AC-3, AC-6.
PE-2(2)	Physical Access Authorizations | Two Forms of Identification	Require two forms of identification from the following forms of identification for visitor access to t	Acceptable forms of identification include passports, REAL ID-compliant drivers' licenses, and Pers	IA-2, IA-4, IA-5.
PE-2(3)	Physical Access Authorizations | Restrict Unescorted Access	Restrict unescorted access to the facility where the system resides to personnel with [Selection (or	Individuals without required security clearances, access approvals, or need to know are escorted b	PS-2, PS-6.
PE-3	Physical Access Control	a. Enforce physical access authorizations at [Assignment: organization-defined entry and exit points to the facility where the system resides] by: 1. Verifying individual access authorizations before granting access to the facility; and 2. Controlling 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.	Physical access control applies to employees and visitors. Individuals with permanent physical acc	AT-3, AU-2, AU-6, AU-9, AU-13, CP-10, IA-3, IA-8, MA-5, MP-2, MP-4, PE-2, PE-4, PE-5, PE-8, PS-2, PS-3, PS-6, PS-7, RA-3, SC-28, SI-4, SR-3.
PE-3(1)	Physical Access Control | System Access	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].	Control of physical access to the system provides additional physical security for those areas within facilities where there is a concentration of system components.	None.
PE-3(2)	Physical Access Control | Facility and Systems	Perform security checks [Assignment: organization-defined frequency] at the physical perimeter o	Organizations determine the extent, frequency, and/or randomness of security checks to adequat	AC-4, SC-7.
PE-3(3)	Physical Access Control | Continuous Guards	Employ guards to control [Assignment: organization-defined physical access points] to the facility	Employing guards at selected physical access points to the facility provides a more rapid response	CP-6, CP-7, PE-6.
PE-3(4)	Physical Access Control | Lockable Casings	Use lockable physical casings to protect [Assignment: organization-defined system components] from unauthorized physical access.	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.	None.
PE-3(5)	Physical Access Control | Tamper Protection	Employ [Assignment: organization-defined anti-tamper technologies] to [Selection (one or more):	Organizations can implement tamper detection and prevention at selected hardware components	SA-16, SR-9, SR-11.
PE-10(1)	Emergency Shutoff | Accidental and Unauthorized Activation	[Withdrawn: Incorporated into PE-10.]		
PE-3(7)	Physical Access Control | Physical Barriers	Limit access using physical barriers.	Physical barriers include bollards, concrete slabs, jersey walls, and hydraulic active vehicle barriers.	None.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
PE-3(8)	Physical Access Control | Access Control Vestibules	Employ access control vestibules at [Assignment: organization-defined locations within the facility].	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).	None.
PE-4	Access Control for Transmission	Control physical access to [Assignment: organization-defined system distribution and transmission	Security controls applied to system distribution and transmission lines prevent accidental damage	AT-3, IA-4, MP-2, MP-4, PE-2, PE-3, PE-5, PE-9, SC-7, SC-8.
PE-5	Access Control for Output Devices	Control physical access to output from [Assignment: organization-defined output devices] to preve	Controlling physical access to output devices includes placing output devices in locked rooms or ot	PE-2, PE-3, PE-4, PE-18.
PE-13(3)	Fire Protection | Automatic Fire Suppression	[Withdrawn: Incorporated into PE-13(2).]		
PE-5(2)	Access Control for Output Devices | Link to Individual Identity	Link individual identity to receipt of output from output devices.	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.	None.
PE-18(1)	Location of System Components | Facility Site	[Withdrawn: Moved to PE-23.]		
PE-6	Monitoring Physical Access	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.	Physical access monitoring includes publicly accessible areas within organizational facilities. Examp	AU-2, AU-6, AU-9, AU-12, CA-7, CP-10, IR-4, IR-8.
PE-6(1)	Monitoring Physical Access | Intrusion Alarms and Surveillance Equipment	Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment.	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.	None.
PE-6(2)	Monitoring Physical Access | Automated Intrusion Recognition and Responses	Recognize [Assignment: organization-defined classes or types of intrusions] and initiate [Assignme	Response actions can include notifying selected organizational personnel or law enforcement pers	SI-4.
PE-6(3)	Monitoring Physical Access | Video Surveillance	(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].	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.	None.
PE-6(4)	Monitoring Physical Access | Monitoring Physical Access to Systems	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].	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.	None.
PE-3(6)	Physical Access Control | Facility Penetration Testing	[Withdrawn: Incorporated into CA-8.]		
PE-8	Visitor Access Records	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].	Visitor access records include the names and organizations of individuals visiting, visitor signatures	PE-2, PE-3, PE-6.
PE-8(1)	Visitor Access Records | Automated Records Maintenance and Review	Maintain and review visitor access records using [Assignment: organization-defined automated mechanisms].	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.	None.
PE-5(1)	Access Control for Output Devices | Access to Output by Authorized Individuals	[Withdrawn: Incorporated into PE-5.]		
PE-8(3)	Visitor Access Records | Limit Personally Identifiable Information Elements	Limit personally identifiable information contained in visitor access records to the following eleme	Organizations may have requirements that specify the contents of visitor access records. Limiting	RA-3, SA-8.
PE-9	Power Equipment and Cabling	Protect power equipment and power cabling for the system from damage and destruction.	Organizations determine the types of protection necessary for the power equipment and cabling	PE-4.
PE-9(1)	Power Equipment and Cabling | Redundant Cabling	Employ redundant power cabling paths that are physically separated by [Assignment: organization-defined distance].	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.	None.
PE-9(2)	Power Equipment and Cabling | Automatic Voltage Controls	Employ automatic voltage controls for [Assignment: organization-defined critical system components].	Automatic voltage controls can monitor and control voltage. Such controls include voltage regulators, voltage conditioners, and voltage stabilizers.	None.
PE-10	Emergency Shutoff	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.	Emergency power shutoff primarily applies to organizational facilities that contain concentrations	PE-15.
PE-5(3)	Access Control for Output Devices | Marking Output Devices	[Withdrawn: Incorporated into PE-22.]		

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
PE-11	Emergency Power	Provide an uninterruptible power supply to facilitate [Selection (one or more): an orderly shutdow	An uninterruptible power supply (UPS) is an electrical system or mechanism that provides emerge	AT-3, CP-2, CP-7.
PE-11(1)	Emergency Power | Alternate Power Supply — Minimal Operational Capability	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.	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.	None.
PE-11(2)	Emergency Power | Alternate Power Supply — Self-contained	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.	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.	None.
PE-12	Emergency Lighting	Employ and maintain automatic emergency lighting for the system that activates in the event of a	The provision of emergency lighting applies primarily to organizational facilities that contain conce	CP-2, CP-7.
PE-12(1)	Emergency Lighting | Essential Mission and Business Functions	Provide emergency lighting for all areas within the facility supporting essential mission and business functions.	Organizations define their essential missions and functions.	None.
PE-13	Fire Protection	Employ and maintain fire detection and suppression systems that are supported by an independe	The provision of fire detection and suppression systems applies primarily to organizational faciliti	AT-3.
PE-13(1)	Fire Protection | Detection Systems — Automatic Activation and Notification	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.	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.	None.
PE-13(2)	Fire Protection | Suppression Systems — Automatic Activation and Notification	(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.	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.	None.
PE-7	Visitor Control	[Withdrawn: Incorporated into PE-2 and PE-3.]		
PE-13(4)	Fire Protection | Inspections	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].	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.	None.
PE-14	Environmental Controls	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].	The provision of environmental controls applies primarily to organizational facilities that contain c	AT-3, CP-2.
PE-14(1)	Environmental Controls | Automatic Controls	Employ the following automatic environmental controls in the facility to prevent fluctuations potentially harmful to the system: [Assignment: organization-defined automatic environmental controls].	The implementation of automatic environmental controls provides an immediate response to environmental conditions that can damage, degrade, or destroy organizational systems or systems components.	None.
PE-14(2)	Environmental Controls | Monitoring with Alarms and Notifications	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].	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.	None.
PE-15	Water Damage Protection	Protect the system from damage resulting from water leakage by providing master shutoff or isola	The provision of water damage protection primarily applies to organizational facilities that contair	AT-3, PE-10.
PE-15(1)	Water Damage Protection | Automation Support	Detect the presence of water near the system and alert [Assignment: organization-defined personnel or roles] using [Assignment: organization-defined automated mechanisms].	Automated mechanisms include notification systems, water detection sensors, and alarms.	None.
PE-16	Delivery and Removal	a. Authorize and control [Assignment: organization-defined types of system components] entering and exiting the facility; and b. Maintain records of the system components.	Enforcing authorizations for entry and exit of system components may require restricting access to	CM-3, CM-8, MA-2, MA-3, MP-5, PE-20, SR-2, SR-3, SR-4, SR-6.
PE-17	Alternate Work Site	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.	Alternate work sites include government facilities or the private residences of employees. While d	AC-17, AC-18, CP-7.
PE-18	Location of System Components	Position system components within the facility to minimize potential damage from [Assignment: o	Physical and environmental hazards include floods, fires, tornadoes, earthquakes, hurricanes, terr	CP-2, PE-5, PE-19, PE-20, RA-3.
PE-8(2)	Visitor Access Records | Physical Access Records	[Withdrawn: Incorporated into PE-2.]		
PE-19	Information Leakage	Protect the system from information leakage due to electromagnetic signals emanations.	Information leakage is the intentional or unintentional release of data or information to an untrus	AC-18, PE-18, PE-20.
PE-19(1)	Information Leakage | National Emissions Policies and Procedures	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.	Emissions Security (EMSEC) policies include the former TEMPEST policies.	None.
PE-20	Asset Monitoring and Tracking	Employ [Assignment: organization-defined asset location technologies] to track and monitor the lo	Asset location technologies can help ensure that critical assets—including vehicles, equipment, an	CM-8, PE-16, PM-8.
PE-21	Electromagnetic Pulse Protection	Employ [Assignment: organization-defined protective measures] against electromagnetic pulse da	An electromagnetic pulse (EMP) is a short burst of electromagnetic energy that is spread over a ra	PE-18, PE-19.
PE-22	Component Marking	Mark [Assignment: organization-defined system hardware components] indicating the impact leve	Hardware components that may require marking include input and output devices. Input devices i	AC-3, AC-4, AC-16, MP-3.
PE-23	Facility Location	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.	Physical and environmental hazards include floods, fires, tornadoes, earthquakes, hurricanes, terr	CP-2, PE-18, PE-19, PM-8, PM-9, RA-3.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
PL-1	Policy and Procedures	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].	Planning policy and procedures for the controls in the PL family implemented within systems and o	PM-9, PS-8, SI-12.
PL-2	System Security and Privacy Plans	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.	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	AC-2, AC-6, AC-14, AC-17, AC-20, CA-2, CA-3, CA-7, CM-9, CM-13, CP-2, CP-4, IR-4, IR-8, MA-4, MA-5, MP-4, MP-5, PL-7, PL-8, PL-10, PL-11, PM-1, PM-7, PM-8, PM-9, PM-10, PM-11, RA-3, RA-8, RA-9, SA-5, SA-17, SA-22, SI-12, SR-2, SR-4.
PL-2(1)	System Security and Privacy Plans | Concept of Operations	[Withdrawn: Incorporated into PL-7.]		
PL-2(2)	System Security and Privacy Plans | Functional Architecture	[Withdrawn: Incorporated into PL-8.]		
PL-2(3)	System Security and Privacy Plans | Plan and Coordinate with Other Organizational Entities	[Withdrawn: Incorporated into PL-2.]		
PL-3	System Security Plan Update	[Withdrawn: Incorporated into PL-2.]		
PL-4	Rules of Behavior	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].	Rules of behavior represent a type of access agreement for organizational users. Other types of ad	AC-2, AC-6, AC-8, AC-9, AC-17, AC-18, AC-19, AC-20, AT-2, AT-3, CM-11, IA-2, IA-4, IA-5, MP-7, PS-6, PS-8, SA-5, SI-12.
PL-4(1)	Rules of Behavior | Social Media and External Site/application Usage Restrictions	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.	Social media, social networking, and external site/application usage restrictions address rules of b	AC-22, AU-13.
PL-5	Privacy Impact Assessment	[Withdrawn: Incorporated into RA-8.]		
PL-6	Security-related Activity Planning	[Withdrawn: Incorporated into PL-2.]		

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
PL-7	Concept of Operations	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].	The CONOPS may be included in the security or privacy plans for the system or in other system de	PL-2, SA-2, SI-12.
PL-8	Security and Privacy Architectures	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.	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	CM-2, CM-6, PL-2, PL-7, PL-9, PM-5, PM-7, RA-9, SA-3, SA-5, SA-8, SA-17, SC-7.
PL-8(1)	Security and Privacy Architectures | Defense in Depth	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.	Organizations strategically allocate security and privacy controls in the security and privacy archite	SC-2, SC-3, SC-29, SC-36.
PL-8(2)	Security and Privacy Architectures | Supplier Diversity	Require that [Assignment: organization-defined controls] allocated to [Assignment: organization-d	Information technology products have different strengths and weaknesses. Providing a broad spe	SC-29, SR-3.
PL-9	Central Management	Centrally manage [Assignment: organization-defined controls and related processes].	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.	PL-8, PM-9.
PL-10	Baseline Selection	Select a control baseline for the system.	Control baselines are predefined sets of controls specifically assembled to address the protection	PL-2, PL-11, RA-2, RA-3, SA-8.
PL-11	Baseline Tailoring	Tailor the selected control baseline by applying specified tailoring actions.	The concept of tailoring allows organizations to specialize or customize a set of baseline controls b	PL-10, RA-2, RA-3, RA-9, SA-8.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
PM-1	Information Security Program Plan	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.	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.	PL-2, PM-18, PM-30, RA-9, SI-12, SR-2.
PM-2	Information Security Program Leadership Role	Appoint a senior agency information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.	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.	None.
PM-3	Information Security and Privacy Resources	a. Include the resources needed to implement the information security and privacy programs in capital planning and investment requests and document all exceptions to this requirement; b. Prepare documentation required for addressing information security and privacy programs in capital planning and investment requests in accordance with applicable laws, executive orders, directives, policies, regulations, standards; and c. Make available for expenditure, the planned information security and privacy resources.	Organizations consider establishing champions for information security and privacy and, as part o	PM-4, SA-2.
PM-4	Plan of Action and Milestones Process	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.	The plan of action and milestones is a key organizational document and is subject to reporting req	CA-5, CA-7, PM-3, RA-7, SI-12.
PM-5	System Inventory	Develop and update [Assignment: organization-defined frequency] an inventory of organizational systems.	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.	None.
PM-5(1)	System Inventory | Inventory of Personally Identifiable Information	Establish, maintain, and update [Assignment: organization-defined frequency] an inventory of all s	An inventory of systems, applications, and projects that process personally identifiable informatio	AC-3, CM-8, CM-12, CM-13, PL-8, PM-22, PT-3, PT-5, SI-12, SI-18.
PM-6	Measures of Performance	Develop, monitor, and report on the results of information security and privacy measures of perfo	Measures of performance are outcome-based metrics used by an organization to measure the eff	CA-7, PM-9.
PM-7	Enterprise Architecture	Develop and maintain an enterprise architecture with consideration for information security, priva	The integration of security and privacy requirements and controls into the enterprise architecture	AU-6, PL-2, PL-8, PM-11, RA-2, SA-3, SA-8, SA-17.
PM-7(1)	Enterprise Architecture | Offloading	Offload [Assignment: organization-defined non-essential functions or services] to other systems, s	Not every function or service that a system provides is essential to organizational mission or busin	SA-8.
PM-8	Critical Infrastructure Plan	Address information security and privacy issues in the development, documentation, and updatin	Protection strategies are based on the prioritization of critical assets and resources. The requirem	CP-2, CP-4, PE-18, PL-2, PM-9, PM-11, PM-18, RA-3, SI-12.
PM-9	Risk Management Strategy	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.	An organization-wide risk management strategy includes an expression of the security and privacy	AC-1, AU-1, AT-1, CA-1, CA-2, CA-5, CA-6, CA-7, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PL-2, PM-2, PM-8, PM-18, PM-28, PM-30, PS-1, PT-1, PT-2, PT-3, RA-1, RA-3, RA-9, SA-1, SA-4, SC-1, SC-38, SI-1, SI-12, SR-1, SR-2.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
PM-10	Authorization Process	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.	Authorization processes for organizational systems and environments of operation require the im	CA-6, CA-7, PL-2.
PM-11	Mission and Business Process Definition	a. Define organizational mission and business processes with consideration for information security and privacy and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and b. Determine information protection and personally identifiable information processing needs arising from the defined mission and business processes; and c. Review and revise the mission and business processes [Assignment: organization-defined frequency].	Protection needs are technology-independent capabilities that are required to counter threats to	CP-2, PL-2, PM-7, PM-8, RA-2, RA-3, RA-9, SA-2.
PM-12	Insider Threat Program	Implement an insider threat program that includes a cross-discipline insider threat incident handli	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.	AC-6, AT-2, AU-6, AU-7, AU-10, AU-12, AU-13, CA-7, IA-4, IR-4, MP-7, PE-2, PM-16, PS-3, PS-4, PS-5, PS-7, PS-8, SC-7, SC-38, SI-4, PM-14.
PM-13	Security and Privacy Workforce	Establish a security and privacy workforce development and improvement program.	Security and privacy workforce development and improvement programs include defining the kno	AT-2, AT-3.
PM-14	Testing, Training, and Monitoring	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.	A process for organization-wide security and privacy testing, training, and monitoring helps ensure	AT-2, AT-3, CA-7, CP-4, IR-3, PM-12, SI-4.
PM-15	Security and Privacy Groups and Associations	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.	Ongoing contact with security and privacy groups and associations is important in an environment	SA-11, SI-5.
PM-16	Threat Awareness Program	Implement a threat awareness program that includes a cross-organization information-sharing ca	Because of the constantly changing and increasing sophistication of adversaries, especially the adv	IR-4, PM-12.
PM-16(1)	Threat Awareness Program | Automated Means for Sharing Threat Intelligence	Employ automated mechanisms to maximize the effectiveness of sharing threat intelligence information.	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.	None.
PM-17	Protecting Controlled Unclassified Information on External Systems	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].	Controlled unclassified information is defined by the National Archives and Records Administratio	CA-6, PM-10.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
PM-18	Privacy Program Plan	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.	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.	PM-8, PM-9, PM-19.
PM-19	Privacy Program Leadership Role	Appoint a senior agency official for privacy with the authority, mission, accountability, and resourc	The privacy officer is an organizational official. For federal agencies—as defined by applicable laws	PM-18, PM-20, PM-23, PM-24, PM-27.
PM-20	Dissemination of Privacy Program Information	Maintain a central resource webpage on the organization's principal public website that serves as a central source of information about the organization's privacy program and that: 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.	For federal agencies, the webpage is located at www.[agency].gov/privacy. Federal agencies includ	AC-3, PM-19, PT-5, PT-6, PT-7, RA-8.
PM-20(1)	Dissemination of Privacy Program Information | Privacy Policies on Websites, Applications, and Digital Services	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.	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.	None.
PM-21	Accounting of Disclosures	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.	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.	AC-3, AU-2, PT-2.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
PM-22	Personally Identifiable Information Quality Management	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.	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.	PM-23, SI-18.
PM-23	Data Governance Body	Establish a Data Governance Body consisting of [Assignment: organization-defined roles] with [As	A Data Governance Body can help ensure that the organization has coherent policies and the abili	AT-2, AT-3, PM-19, PM-22, PM-24, PT-7, SI-4, SI-19.
PM-24	Data Integrity Board	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.	A Data Integrity Board is the board of senior officials designated by the head of a federal agency a	AC-4, PM-19, PM-23, PT-2, PT-8.
PM-25	Minimization of Personally Identifiable Information Used in Testing, Training, and Research	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].	The use of personally identifiable information in testing, research, and training increases the risk o	PM-23, PT-3, SA-3, SA-8, SI-12.
PM-26	Complaint Management	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].	Complaints, concerns, and questions from individuals can serve as valuable sources of input to or	IR-7, IR-9, PM-22, SI-18.
PM-27	Privacy Reporting	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].	Through internal and external reporting, organizations promote accountability and transparency i	IR-9, PM-19.
PM-28	Risk Framing	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].	Risk framing is most effective when conducted at the organization level and in consultation with st	CA-7, PM-9, RA-3, RA-7.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
PM-29	Risk Management Program Leadership Roles	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.	The senior accountable official for risk management leads the risk executive (function) in organiza	PM-2, PM-19.
PM-30	Supply Chain Risk Management Strategy	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.	An organization-wide supply chain risk management strategy includes an unambiguous expressio	CM-10, PM-9, SR-1, SR-2, SR-3, SR-4, SR-5, SR-6, SR-7, SR-8, SR-9, SR-11.
PM-30(1)	Supply Chain Risk Management Strategy | Suppliers of Critical or Mission-essential Items	Identify, prioritize, and assess suppliers of critical or mission-essential technologies, products, and	The identification and prioritization of suppliers of critical or mission-essential technologies, produ	RA-3, SR-6.
PM-31	Continuous Monitoring Strategy	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].	Continuous monitoring at the organization level facilitates ongoing awareness of the security and	AC-2, AC-6, AC-17, AT-4, AU-6, AU-13, CA-2, CA-5, CA-6, CA-7, CM-3, CM-4, CM-6, CM-11, IA-5, IR-5, MA-2, MA-3, MA-4, PE-3, PE-6, PE-14, PE-16, PE-20, PL-2, PM-4, PM-6, PM-9, PM-10, PM-12, PM-14, PM-23, PM-28, PS-7, PT-7, RA-3, RA-5, RA-7, SA-9, SA-11, SC-5, SC-7, SC-18, SC-38, SC-43, SI-3, SI-4, SI-12, SR-2, SR-4.
PM-32	Purposing	Analyze [Assignment: organization-defined systems or systems components] supporting mission e	Systems are designed to support a specific mission or business function. However, over time, syst	CA-7, PL-2, RA-3, RA-9.
PS-1	Policy and Procedures	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].	Personnel security policy and procedures for the controls in the PS family that are implemented w	PM-9, PS-8, SI-12.
PS-2	Position Risk Designation	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].	Position risk designations reflect Office of Personnel Management (OPM) policy and guidance. Pro	AC-5, AT-3, PE-2, PE-3, PL-2, PS-3, PS-6, SA-5, SA-21, SI-12.
PS-3	Personnel Screening	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].	Personnel screening and rescreening activities reflect applicable laws, executive orders, directives,	AC-2, IA-4, MA-5, PE-2, PM-12, PS-2, PS-6, PS-7, SA-21.
PS-3(1)	Personnel Screening | Classified Information	Verify that individuals accessing a system processing, storing, or transmitting classified informatio	Classified information is the most sensitive information that the Federal Government processes, s	AC-3, AC-4.
PS-3(2)	Personnel Screening | Formal Indoctrination	Verify that individuals accessing a system processing, storing, or transmitting types of classified inf	Types of classified information that require formal indoctrination include Special Access Program (	AC-3, AC-4.
PS-3(3)	Personnel Screening | Information Requiring Special Protective Measures	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].	Organizational information that requires special protection includes controlled unclassified information. Personnel security criteria include position sensitivity background screening requirements.	None.
PS-3(4)	Personnel Screening | Citizenship Requirements	Verify that individuals accessing a system processing, storing, or transmitting [Assignment: organization-defined information types] meet [Assignment: organization-defined citizenship requirements].	None.	None.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
PS-4	Personnel Termination	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.	System property includes hardware authentication tokens, system administration technical manua	AC-2, IA-4, PE-2, PM-12, PS-6, PS-7.
PS-4(1)	Personnel Termination | Post-employment Requirements	(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.	Organizations consult with the Office of the General Counsel regarding matters of post-employment requirements on terminated individuals.	None.
PS-4(2)	Personnel Termination | Automated Actions	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].	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.	None.
PS-5	Personnel Transfer	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].	Personnel transfer applies when reassignments or transfers of individuals are permanent or of su	AC-2, IA-4, PE-2, PM-12, PS-4, PS-7.
PS-6	Access Agreements	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].	Access agreements include nondisclosure agreements, acceptable use agreements, rules of behav	AC-17, PE-2, PL-4, PS-2, PS-3, PS-6, PS-7, PS-8, SA-21, SI-12.
PS-6(1)	Access Agreements | Information Requiring Special Protection	[Withdrawn: Incorporated into PS-3.]		
PS-6(2)	Access Agreements | Classified Information Requiring Special Protection	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.	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.	None.
PS-6(3)	Access Agreements | Post-employment Requirements	(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.	Organizations consult with the Office of the General Counsel regarding matters of post-employme	PS-4.
PS-7	External Personnel Security	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.	External provider refers to organizations other than the organization operating or acquiring the sy	AT-2, AT-3, MA-5, PE-3, PS-2, PS-3, PS-4, PS-5, PS-6, SA-5, SA-9, SA-21.
PS-8	Personnel Sanctions	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.	Organizational sanctions reflect applicable laws, executive orders, directives, regulations, policies,	PL-4, PM-12, PS-6, PT-1.
PS-9	Position Descriptions	Incorporate security and privacy roles and responsibilities into organizational position descriptions.	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.	None.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
PT-1	Policy and Procedures	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].	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.	None.
PT-2	Authority to Process Personally Identifiable Information	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.	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.	AC-2, AC-3, CM-13, IR-9, PM-9, PM-24, PT-1, PT-3, PT-5, PT-6, RA-3, RA-8, SI-12, SI-18.
PT-2(1)	Authority to Process Personally Identifiable Information | Data Tagging	Attach data tags containing [Assignment: organization-defined authorized processing] to [Assignm	Data tags support the tracking and enforcement of authorized processing by conveying the types	AC-16, CA-6, CM-12, PM-5, PM-22, PT-4, SC-16, SC-43, SI-10, SI-15, SI-19.
PT-2(2)	Authority to Process Personally Identifiable Information | Automation	Manage enforcement of the authorized processing of personally identifiable information using [A	Automated mechanisms augment verification that only authorized processing is occurring.	CA-6, CM-12, PM-5, PM-22, PT-4, SC-16, SC-43, SI-10, SI-15, SI-19.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
PT-3	Personally Identifiable Information Processing Purposes	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].	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.	AC-2, AC-3, AT-3, CM-13, IR-9, PM-9, PM-25, PT-2, PT-5, PT-6, PT-7, RA-8, SC-43, SI-12, SI-18.
PT-3(1)	Personally Identifiable Information Processing Purposes | Data Tagging	Attach data tags containing the following purposes to [Assignment: organization-defined elements	Data tags support the tracking of processing purposes by conveying the purposes along with the r	CA-6, CM-12, PM-5, PM-22, SC-16, SC-43, SI-10, SI-15, SI-19.
PT-3(2)	Personally Identifiable Information Processing Purposes | Automation	Track processing purposes of personally identifiable information using [Assignment: organization-	Automated mechanisms augment tracking of the processing purposes.	CA-6, CM-12, PM-5, PM-22, SC-16, SC-43, SI-10, SI-15, SI-19.
PT-4	Consent	Implement [Assignment: organization-defined tools or mechanisms] for individuals to consent to t	Consent allows individuals to participate in making decisions about the processing of their informa	AC-16, PT-2, PT-5.
PT-4(1)	Consent | Tailored Consent	Provide [Assignment: organization-defined mechanisms] to allow individuals to tailor processing p	While some processing may be necessary for the basic functionality of the product or service, othe	PT-2.
PT-4(2)	Consent | Just-in-time Consent	Present [Assignment: organization-defined consent mechanisms] to individuals at [Assignment: or	Just-in-time consent enables individuals to participate in how their personally identifiable informa	PT-2.
PT-4(3)	Consent | Revocation	Implement [Assignment: organization-defined tools or mechanisms] for individuals to revoke cons	Revocation of consent enables individuals to exercise control over their initial consent decision wh	PT-2.
PT-5	Privacy Notice	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].	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.	PM-20, PM-22, PT-2, PT-3, PT-4, PT-7, RA-3, SC-42, SI-18.
PT-5(1)	Privacy Notice | Just-in-time Notice	Present notice of personally identifiable information processing to individuals at a time and locatio	Just-in-time notices inform individuals of how organizations process their personally identifiable i	PM-21.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
PT-5(2)	Privacy Notice | Privacy Act Statements	Include Privacy Act statements on forms that collect information that will be maintained in a Priva	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.	PT-6.
PT-6	System of Records Notice	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.	The PRIVACT requires that federal agencies publish a system of records notice in the Federal Regis	AC-3, PM-20, PT-2, PT-3, PT-5.
PT-6(1)	System of Records Notice | Routine Uses	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.	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.	None.
PT-6(2)	System of Records Notice | Exemption Rules	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.	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.	None.
PT-7	Specific Categories of Personally Identifiable Information	Apply [Assignment: organization-defined processing conditions] for specific categories of personal	Organizations apply any conditions or protections that may be necessary for specific categories of	IR-9, PT-2, PT-3, RA-3.
PT-7(1)	Specific Categories of Personally Identifiable Information | Social Security Numbers	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.	Federal law and policy establish specific requirements for organizations' processing of Social Secur	IA-4.
PT-7(2)	Specific Categories of Personally Identifiable Information | First Amendment Information	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.	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.	None.
PT-8	Computer Matching Requirements	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.	The PRIVACT establishes requirements for federal and non-federal agencies if they engage in a ma	PM-24.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
RA-1	Policy and Procedures	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].	Risk assessment policy and procedures address the controls in the RA family that are implemented	PM-9, PS-8, SI-12.
RA-2	Security Categorization	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.	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.	CM-8, MP-4, PL-2, PL-10, PL-11, PM-7, RA-3, RA-5, RA-7, RA-8, SA-8, SC-7, SC-38, SI-12.
RA-2(1)	Security Categorization | Impact-level Prioritization	Conduct an impact-level prioritization of organizational systems to obtain additional granularity on system impact levels.	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.	None.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
RA-3	Risk Assessment	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.	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.	CA-3, CA-6, CM-4, CM-13, CP-6, CP-7, IA-8, MA-5, PE-3, PE-8, PE-18, PL-2, PL-10, PL-11, PM-8, PM-9, PM-28, PT-2, PT-7, RA-2, RA-5, RA-7, SA-8, SA-9, SC-38, SI-12.
RA-3(1)	Risk Assessment | Supply Chain Risk Assessment	(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.	Supply chain-related events include disruption, use of defective components, insertion of countert	RA-2, RA-9, PM-17, PM-30, SR-2.
RA-3(2)	Risk Assessment | Use of All-source Intelligence	Use all-source intelligence to assist in the analysis of risk.	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.	None.
RA-3(3)	Risk Assessment | Dynamic Threat Awareness	Determine the current cyber threat environment on an ongoing basis using [Assignment: organiza	The threat awareness information that is gathered feeds into the organization's information secur	AT-2.
RA-3(4)	Risk Assessment | Predictive Cyber Analytics	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].	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.	None.
RA-4	Risk Assessment Update	[Withdrawn: Incorporated into RA-3.]		

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
RA-5	Vulnerability Monitoring and Scanning	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.	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	CA-2, CA-7, CA-8, CM-2, CM-4, CM-6, CM-8, RA-2, RA-3, SA-11, SA-15, SC-38, SI-2, SI-3, SI-4, SI-7, SR-11.
RA-5(1)	Vulnerability Monitoring and Scanning | Update Tool Capability	[Withdrawn: Incorporated into RA-5.]		
RA-5(2)	Vulnerability Monitoring and Scanning | Update Vulnerabilities to Be Scanned	Update the system vulnerabilities to be scanned [Selection (one or more): [Assignment: organizati	Due to the complexity of modern software, systems, and other factors, new vulnerabilities are dis	SI-5.
RA-5(3)	Vulnerability Monitoring and Scanning | Breadth and Depth of Coverage	Define the breadth and depth of vulnerability scanning coverage.	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.	None.
RA-5(4)	Vulnerability Monitoring and Scanning | Discoverable Information	Determine information about the system that is discoverable and take [Assignment: organization-	Discoverable information includes information that adversaries could obtain without compromisi	AU-13, SC-26.
RA-5(5)	Vulnerability Monitoring and Scanning | Privileged Access	Implement privileged access authorization to [Assignment: organization-defined system components] for [Assignment: organization-defined vulnerability scanning activities].	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.	None.
RA-5(6)	Vulnerability Monitoring and Scanning | Automated Trend Analyses	Compare the results of multiple vulnerability scans using [Assignment: organization-defined automated mechanisms].	Using automated mechanisms to analyze multiple vulnerability scans over time can help determine trends in system vulnerabilities and identify patterns of attack.	None.
RA-5(7)	Vulnerability Monitoring and Scanning | Automated Detection and Notification of Unauthorized Components	[Withdrawn: Incorporated into CM-8.]		
RA-5(8)	Vulnerability Monitoring and Scanning | Review Historic Audit Logs	Review historic audit logs to determine if a vulnerability identified in a [Assignment: organization-	Reviewing historic audit logs to determine if a recently detected vulnerability in a system has been	AU-6, AU-11.
RA-5(9)	Vulnerability Monitoring and Scanning | Penetration Testing and Analyses	[Withdrawn: Incorporated into CA-8.]		
RA-5(10)	Vulnerability Monitoring and Scanning | Correlate Scanning Information	Correlate the output from vulnerability scanning tools to determine the presence of multi-vulnerability and multi-hop attack vectors.	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.	None.
RA-5(11)	Vulnerability Monitoring and Scanning | Public Disclosure Program	Establish a public reporting channel for receiving reports of vulnerabilities in organizational systems and system components.	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.	None.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
RA-6	Technical Surveillance Countermeasures Survey	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]].	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.	None.
RA-7	Risk Response	Respond to findings from security and privacy assessments, monitoring, and audits in accordance	Organizations have many options for responding to risk including mitigating risk by implementing	CA-5, IR-9, PM-4, PM-28, RA-2, RA-3, SR-2.
RA-8	Privacy Impact Assessments	Conduct privacy impact assessments for systems, programs, or other activities before: a. Developing or procuring information technology that processes personally identifiable information; and b. 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.	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.	CM-4, CM-9, CM-13, PT-2, PT-3, PT-5, RA-1, RA-2, RA-3, RA-7.
RA-9	Criticality Analysis	Identify critical system components and functions by performing a criticality analysis for [Assignme	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.	CP-2, PL-2, PL-8, PL-11, PM-1, PM-11, RA-2, SA-8, SA-15, SA-20, SR-5.
RA-10	Threat Hunting	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].	Threat hunting is an active means of cyber defense in contrast to traditional protection measures,	CA-2, CA-7, CA-8, RA-3, RA-5, RA-6, SI-4.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
SA-1	Policy and Procedures	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].	System and services acquisition policy and procedures address the controls in the SA family that a	PM-9, PS-8, SA-8, SI-12.
SA-2	Allocation of Resources	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.	Resource allocation for information security and privacy includes funding for system and services	PL-7, PM-3, PM-11, SA-9, SR-3, SR-5.
SA-3	System Development Life Cycle	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.	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.	AT-3, PL-8, PM-7, SA-4, SA-5, SA-8, SA-11, SA-15, SA-17, SA-22, SR-3, SR-4, SR-5, SR-9.
SA-3(1)	System Development Life Cycle | Manage Preproduction Environment	Protect system preproduction environments commensurate with risk throughout the system deve	The preproduction environment includes development, test, and integration environments. The p	CM-2, CM-4, RA-3, RA-9, SA-4.
SA-3(2)	System Development Life Cycle | Use of Live or Operational Data	(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.	Live data is also referred to as operational data. The use of live or operational data in preproducti	PM-25, RA-3.
SA-3(3)	System Development Life Cycle | Technology Refresh	Plan for and implement a technology refresh schedule for the system throughout the system deve	Technology refresh planning may encompass hardware, software, firmware, processes, personne	MA-6.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
SA-4	Acquisition Process	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.	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.	CM-6, CM-8, PS-7, SA-3, SA-5, SA-8, SA-11, SA-15, SA-16, SA-17, SA-21, SR-3, SR-5.
SA-4(1)	Acquisition Process | Functional Properties of Controls	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.	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.	None.
SA-4(2)	Acquisition Process | Design and Implementation Information for Controls	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].	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.	None.
SA-4(3)	Acquisition Process | Development Methods, Techniques, and Practices	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].	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.	None.
SA-12	Supply Chain Protection	[Withdrawn: Incorporated into SR Family.]		
SA-4(5)	Acquisition Process | System, Component, and Service Configurations	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.	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.	None.
SA-4(6)	Acquisition Process | Use of Information Assurance Products	(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.	Commercial off-the-shelf IA or IA-enabled information technology products used to protect classif	SC-8, SC-12, SC-13.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
SA-4(7)	Acquisition Process | NIAP-approved Protection Profiles	(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.	See NIAP CCEVS for additional information on NIAP. See NIST CMVP for additional information on	IA-7, SC-12, SC-13.
SA-4(8)	Acquisition Process | Continuous Monitoring Plan for Controls	Require the developer of the system, system component, or system service to produce a plan for	The objective of continuous monitoring plans is to determine if the planned, required, and deploy	CA-7.
SA-4(9)	Acquisition Process | Functions, Ports, Protocols, and Services in Use	Require the developer of the system, system component, or system service to identify the functio	The identification of functions, ports, protocols, and services early in the system development life	CM-7, SA-9.
SA-4(10)	Acquisition Process | Use of Approved PIV Products	Employ only information technology products on the FIPS 201-approved products list for Personal	Products on the FIPS 201-approved products list meet NIST requirements for Personal Identity Ver	IA-2, IA-8, PM-9.
SA-4(11)	Acquisition Process | System of Records	Include [Assignment: organization-defined Privacy Act requirements] in the acquisition contract fo	When, by contract, an organization provides for the operation of a system of records to accomplis	PT-6.
SA-4(12)	Acquisition Process | Data Ownership	(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].	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.	None.
SA-5	System Documentation	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].	System documentation helps personnel understand the implementation and operation of control	CM-4, CM-6, CM-7, CM-8, PL-2, PL-4, PL-8, PS-2, SA-3, SA-4, SA-8, SA-9, SA-10, SA-11, SA-15, SA-16, SA-17, SI-12, SR-3.
SA-12(1)	Supply Chain Protection | Acquisition Strategies / Tools / Methods	[Withdrawn: Moved to SR-5.]		
SA-12(10)	Supply Chain Protection | Validate as Genuine and Not Altered	[Withdrawn: Moved to SR-4(3).]		
SA-12(11)	Supply Chain Protection | Penetration Testing / Analysis of Elements, Processes, and Actors	[Withdrawn: Moved to SR-6(1).]		
SA-12(12)	Supply Chain Protection | Inter-organizational Agreements	[Withdrawn: Moved to SR-8.]		
SA-12(13)	Supply Chain Protection | Critical Information System Components	[Withdrawn: Incorporated into MA-6 and RA-9.]		
SA-12(14)	Supply Chain Protection | Identity and Traceability	[Withdrawn: Moved to SR-4(1) and SR-4(2).]		
SA-12(15)	Supply Chain Protection | Processes to Address Weaknesses or Deficiencies	[Withdrawn: Incorporated into SR-3.]		
SA-8	Security and Privacy Engineering Principles	Apply the following systems security and privacy engineering principles in the specification, design	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.	PL-8, PM-7, RA-2, RA-3, RA-9, SA-3, SA-4, SA-15, SA-17, SA-20, SC-2, SC-3, SC-32, SC-39, SR-2, SR-3, SR-4, SR-5.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
SA-8(1)	Security and Privacy Engineering Principles | Clear Abstractions	Implement the security design principle of clear abstractions.	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.	None.
SA-8(2)	Security and Privacy Engineering Principles | Least Common Mechanism	Implement the security design principle of least common mechanism in [Assignment: organization-defined systems or system components].	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.	None.
SA-8(3)	Security and Privacy Engineering Principles | Modularity and Layering	Implement the security design principles of modularity and layering in [Assignment: organization-	The principles of modularity and layering are fundamental across system engineering disciplines.	SC-2, SC-3.
SA-8(4)	Security and Privacy Engineering Principles | Partially Ordered Dependencies	Implement the security design principle of partially ordered dependencies in [Assignment: organization-defined systems or system components].	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.	None.
SA-8(5)	Security and Privacy Engineering Principles | Efficiently Mediated Access	Implement the security design principle of efficiently mediated access in [Assignment: organizatio	The principle of efficiently mediated access states that policy enforcement mechanisms utilize the	AC-25.
SA-8(6)	Security and Privacy Engineering Principles | Minimized Sharing	Implement the security design principle of minimized sharing in [Assignment: organization-define	The principle of minimized sharing states that no computer resource is shared between system co	SC-31.
SA-8(7)	Security and Privacy Engineering Principles | Reduced Complexity	Implement the security design principle of reduced complexity in [Assignment: organization-defined systems or system components].	The principle of reduced complexity states that the system design is as simple and small as possible. A small and simple design is more understandable, more 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.	None.
SA-8(8)	Security and Privacy Engineering Principles | Secure Evolvability	Implement the security design principle of secure evolvability in [Assignment: organization-define	The principle of secure evolvability states that a system is developed to facilitate the maintenance	CM-3.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
SA-8(9)	Security and Privacy Engineering Principles | Trusted Components	Implement the security design principle of trusted components in [Assignment: organization-defined systems or system components].	The principle of trusted components states that a component is trustworthy to 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.	None.
SA-8(10)	Security and Privacy Engineering Principles | Hierarchical Trust	Implement the security design principle of hierarchical trust in [Assignment: organization-defined systems or system components].	The principle of hierarchical trust for components builds on the principle of trusted components and states that the security dependencies in a system will form a partial ordering if they preserve the principle of trusted components. The partial ordering provides the basis for trustworthiness reasoning or 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.	None.
SA-8(11)	Security and Privacy Engineering Principles | Inverse Modification Threshold	Implement the security design principle of inverse modification threshold in [Assignment: organization-defined systems or system components].	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).	None.
SA-8(12)	Security and Privacy Engineering Principles | Hierarchical Protection	Implement the security design principle of hierarchical protection in [Assignment: organization-defined systems or system components].	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.	None.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
SA-8(13)	Security and Privacy Engineering Principles | Minimized Security Elements	Implement the security design principle of minimized security elements in [Assignment: organization-defined systems or system components].	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.	None.
SA-8(14)	Security and Privacy Engineering Principles | Least Privilege	Implement the security design principle of least privilege in [Assignment: organization-defined sys	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.	AC-6, CM-7.
SA-8(15)	Security and Privacy Engineering Principles | Predicate Permission	Implement the security design principle of predicate permission in [Assignment: organization-defi	The principle of predicate permission states that system designers consider requiring multiple aut	AC-5.
SA-8(16)	Security and Privacy Engineering Principles | Self-reliant Trustworthiness	Implement the security design principle of self-reliant trustworthiness in [Assignment: organization-defined systems or system components].	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.	None.
SA-8(17)	Security and Privacy Engineering Principles | Secure Distributed Composition	Implement the security design principle of secure distributed composition in [Assignment: organization-defined systems or system components].	The principle of secure distributed composition states that the composition of distributed components that enforce the same system security policy 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.	None.
SA-8(18)	Security and Privacy Engineering Principles | Trusted Communications Channels	Implement the security design principle of trusted communications channels in [Assignment: orga	The principle of trusted communication channels states that when composing a system where the	SC-8, SC-12, SC-13.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
SA-8(19)	Security and Privacy Engineering Principles | Continuous Protection	Implement the security design principle of continuous protection in [Assignment: organization-def	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	AC-25.
SA-8(20)	Security and Privacy Engineering Principles | Secure Metadata Management	Implement the security design principle of secure metadata management in [Assignment: organization-defined systems or system components].	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.	None.
SA-8(21)	Security and Privacy Engineering Principles | Self-analysis	Implement the security design principle of self-analysis in [Assignment: organization-defined syste	The principle of self-analysis states that a system component is able to assess its internal state and	CA-7.
SA-8(22)	Security and Privacy Engineering Principles | Accountability and Traceability	Implement the security design principle of accountability and traceability in [Assignment: organiza	The principle of accountability and traceability states that it is possible to trace security-relevant a	AC-6, AU-2, AU-3, AU-6, AU-9, AU-10, AU-12, IA-2, IR-4.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
SA-8(23)	Security and Privacy Engineering Principles | Secure Defaults	Implement the security design principle of secure defaults in [Assignment: organization-defined sy	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.	CM-2, CM-6, SA-4.
SA-8(24)	Security and Privacy Engineering Principles | Secure Failure and Recovery	Implement the security design principle of secure failure and recovery in [Assignment: organizatio	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.	CP-10, CP-12, SC-7, SC-8, SC-24, SI-13.
SA-8(25)	Security and Privacy Engineering Principles | Economic Security	Implement the security design principle of economic security in [Assignment: organization-defined	The principle of economic security states that security mechanisms are not costlier than the poten	RA-3.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
SA-8(26)	Security and Privacy Engineering Principles | Performance Security	Implement the security design principle of performance security in [Assignment: organization-defi	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.	SC-12, SC-13, SI-2, SI-7.
SA-8(27)	Security and Privacy Engineering Principles | Human Factored Security	Implement the security design principle of human factored security in [Assignment: organization-defined systems or system components].	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.	None.
SA-8(28)	Security and Privacy Engineering Principles | Acceptable Security	Implement the security design principle of acceptable security in [Assignment: organization-defined systems or system components].	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.	None.
SA-8(29)	Security and Privacy Engineering Principles | Repeatable and Documented Procedures	Implement the security design principle of repeatable and documented procedures in [Assignmen	The principle of repeatable and documented procedures states that the techniques and methods	CM-1, SA-1, SA-10, SA-11, SA-15, SA-17, SC-1, SI-1.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
SA-8(30)	Security and Privacy Engineering Principles | Procedural Rigor	Implement the security design principle of procedural rigor in [Assignment: organization-defined systems or system components].	The principle of procedural rigor states that the rigor of a system life cycle process is commensurate with its intended trustworthiness. Procedural rigor defines the scope, depth, and detail of the system life cycle procedures. Rigorous system life cycle procedures contribute to the assurance that the system is correct and free of unintended functionality in several ways. First, the procedures impose checks and balances on the life cycle process such that the introduction of 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.	None.
SA-8(31)	Security and Privacy Engineering Principles | Secure System Modification	Implement the security design principle of secure system modification in [Assignment: organizatio	The principle of secure system modification states that system modification maintains system secu	CM-3, CM-4.
SA-8(32)	Security and Privacy Engineering Principles | Sufficient Documentation	Implement the security design principle of sufficient documentation in [Assignment: organization-	The principle of sufficient documentation states that organizational personnel with responsibilitie	AT-2, AT-3, SA-5.
SA-8(33)	Security and Privacy Engineering Principles | Minimization	Implement the privacy principle of minimization using [Assignment: organization-defined processe	The principle of minimization states that organizations should only process personally identifiable	PE-8, PM-25, SC-42, SI-12.
SA-9	External System Services	a. Require that providers of external system services comply with organizational security and privacy requirements and employ the following controls: [Assignment: organization-defined controls]; b. Define and document organizational oversight and user roles and responsibilities with regard to external system services; and c. Employ the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis: [Assignment: organization-defined processes, methods, and techniques].	External system services are provided by an external provider, and the organization has no direct	AC-20, CA-3, CP-2, IR-4, IR-7, PL-10, PL-11, PS-7, SA-2, SA-4, SR-3, SR-5.
SA-9(1)	External System Services | Risk Assessments and Organizational Approvals	(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].	Information security services include the operation of security devices, such as firewalls or key ma	CA-6, RA-3, RA-8.
SA-9(2)	External System Services | Identification of Functions, Ports, Protocols, and Services	Require providers of the following external system services to identify the functions, ports, protoc	Information from external service providers regarding the specific functions, ports, protocols, and	CM-6, CM-7.
SA-9(3)	External System Services | Establish and Maintain Trust Relationship with Providers	Establish, document, and maintain trust relationships with external service providers based on the	Trust relationships between organizations and external service providers reflect the degree of con	SR-2.
SA-9(4)	External System Services | Consistent Interests of Consumers and Providers	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].	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.	None.
SA-9(5)	External System Services | Processing, Storage, and Service Location	Restrict the location of [Selection (one or more): information processing; information or data; syst	The location of information processing, information and data storage, or system services can have	SA-5, SR-4.
SA-9(6)	External System Services | Organization-controlled Cryptographic Keys	Maintain exclusive control of cryptographic keys for encrypted material stored or transmitted thro	Maintaining exclusive control of cryptographic keys in an external system prevents decryption of	SC-12, SC-13, SI-4.
SA-9(7)	External System Services | Organization-controlled Integrity Checking	Provide the capability to check the integrity of information while it resides in the external system.	Storage of organizational information in an external system could limit visibility into the security st	SI-7.
SA-9(8)	External System Services | Processing and Storage Location — U.S. Jurisdiction	Restrict the geographic location of information processing and data storage to facilities located wit	The geographic location of information processing and data storage can have a direct impact on th	SA-5, SR-4.
SA-10	Developer Configuration Management	Require the developer of the system, system component, or system service to: a. Perform configuration management during system, component, or service [Selection (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].	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.	CM-2, CM-3, CM-4, CM-7, CM-9, SA-4, SA-5, SA-8, SA-15, SI-2, SR-3, SR-4, SR-5, SR-6.
SA-10(1)	Developer Configuration Management | Software and Firmware Integrity Verification	Require the developer of the system, system component, or system service to enable integrity ver	Software and firmware integrity verification allows organizations to detect unauthorized changes	SI-7, SR-11.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
SA-10(2)	Developer Configuration Management | Alternative Configuration Management Processes	Provide an alternate configuration management process using organizational personnel in the absence of a dedicated developer configuration management team.	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.	None.
SA-10(3)	Developer Configuration Management | Hardware Integrity Verification	Require the developer of the system, system component, or system service to enable integrity ver	Hardware integrity verification allows organizations to detect unauthorized changes to hardware	SI-7.
SA-10(4)	Developer Configuration Management | Trusted Generation	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.	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.	None.
SA-10(5)	Developer Configuration Management | Mapping Integrity for Version Control	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.	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.	None.
SA-10(6)	Developer Configuration Management | Trusted Distribution	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.	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.	None.
SA-10(7)	Developer Configuration Management | Security and Privacy Representatives	Require [Assignment: organization-defined security and privacy representatives] to be included in the [Assignment: organization-defined configuration change management and control process].	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.	None.
SA-11	Developer Testing and Evaluation	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.	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.	CA-2, CA-7, CM-4, SA-3, SA-4, SA-5, SA-8, SA-15, SA-17, SI-2, SR-5, SR-6, SR-7.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
SA-11(1)	Developer Testing and Evaluation | Static Code Analysis	Require the developer of the system, system component, or system service to employ static code analysis tools to identify common flaws and document the results of the analysis.	Static code analysis provides a technology and methodology for security reviews and includes checking for weaknesses in the code 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.	None.
SA-11(2)	Developer Testing and Evaluation | Threat Modeling and Vulnerability Analyses	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].	Systems, system components, and system services may deviate significantly from the functional ar	PM-15, RA-3, RA-5.
SA-11(3)	Developer Testing and Evaluation | Independent Verification of Assessment Plans and Eviden	(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.	Independent agents have the qualifications—including the expertise, skills, training, certifications,	AT-3, RA-5.
SA-11(4)	Developer Testing and Evaluation | Manual Code Reviews	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].	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.	None.
SA-11(5)	Developer Testing and Evaluation | Penetration Testing	Require the developer of the system, system component, or system service to perform penetration testing: (a) At the following level of rigor: [Assignment: organization-defined breadth and depth of testing]; and (b) Under the following constraints: [Assignment: organization-defined constraints].	Penetration testing is an assessment methodology in which assessors, using all available informati	CA-8, PM-14, PM-25, PT-2, SA-3, SI-2, SI-6.
SA-11(6)	Developer Testing and Evaluation | Attack Surface Reviews	Require the developer of the system, system component, or system service to perform attack surf	Attack surfaces of systems and system components are exposed areas that make those systems m	SA-15.
SA-11(7)	Developer Testing and Evaluation | Verify Scope of Testing and Evaluation	Require the developer of the system, system component, or system service to verify that the scope	Verifying that testing and evaluation provides complete coverage of required controls can be acco	SA-15.
SA-11(8)	Developer Testing and Evaluation | Dynamic Code Analysis	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.	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).	None.
SA-11(9)	Developer Testing and Evaluation | Interactive Application Security Testing	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.	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.	None.
SA-12(2)	Supply Chain Protection | Supplier Reviews	[Withdrawn: Moved to SR-6.]		
SA-12(3)	Supply Chain Protection | Trusted Shipping and Warehousing	[Withdrawn: Incorporated into SR-3.]		

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
SA-12(4)	Supply Chain Protection | Diversity of Suppliers	[Withdrawn: Moved to SR-3(1).]		
SA-12(5)	Supply Chain Protection | Limitation of Harm	[Withdrawn: Moved to SR-3(2).]		
SA-12(6)	Supply Chain Protection | Minimizing Procurement Time	[Withdrawn: Incorporated into SR-5(1).]		
SA-12(7)	Supply Chain Protection | Assessments Prior to Selection / Acceptance / Update	[Withdrawn: Moved to SR-5(2).]		
SA-12(8)	Supply Chain Protection | Use of All-source Intelligence	[Withdrawn: Incorporated into RA-3(2).]		
SA-12(9)	Supply Chain Protection | Operations Security	[Withdrawn: Moved to SR-7.]		
SA-13	Trustworthiness	[Withdrawn: Incorporated into SA-8.]		
SA-14	Criticality Analysis	[Withdrawn: Incorporated into RA-9.]		
SA-14(1)	Criticality Analysis | Critical Components with No Viable Alternative Sourcing	[Withdrawn: Incorporated into SA-20.]		
SA-15(4)	Development Process, Standards, and Tools | Threat Modeling and Vulnerability Analysis	[Withdrawn: Incorporated into SA-11(2).]		
SA-15(9)	Development Process, Standards, and Tools | Use of Live Data	[Withdrawn: Incorporated into SA-3(2).]		
SA-18	Tamper Resistance and Detection	[Withdrawn: Moved to SR-9.]		
SA-18(1)	Tamper Resistance and Detection | Multiple Phases of System Development Life Cycle	[Withdrawn: Moved to SR-9(1).]		
SA-18(2)	Tamper Resistance and Detection | Inspection of Systems or Components	[Withdrawn: Moved to SR-10.]		
SA-19	Component Authenticity	[Withdrawn: Moved to SR-11.]		
SA-19(1)	Component Authenticity | Anti-counterfeit Training	[Withdrawn: Moved to SR-11(1).]		
SA-19(2)	Component Authenticity | Configuration Control for Component Service and Repair	[Withdrawn: Moved to SR-11(2).]		
SA-15	Development Process, Standards, and Tools	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].	Development tools include programming languages and computer-aided design systems. Reviews	MA-6, SA-3, SA-4, SA-8, SA-10, SA-11, SR-3, SR-4, SR-5, SR-6, SR-9.
SA-15(1)	Development Process, Standards, and Tools | Quality Metrics	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].	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.	None.
SA-15(2)	Development Process, Standards, and Tools | Security and Privacy Tracking Tools	Require the developer of the system, system component, or system service to select and employ s	System development teams select and deploy security and privacy tracking tools, including vulnera	SA-11.
SA-15(3)	Development Process, Standards, and Tools | Criticality Analysis	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].	Criticality analysis performed by the developer provides input to the criticality analysis performed	RA-9.
SA-19(3)	Component Authenticity | Component Disposal	[Withdrawn: Moved to SR-12.]		
SA-15(5)	Development Process, Standards, and Tools | Attack Surface Reduction	Require the developer of the system, system component, or system service to reduce attack surfa	Attack surface reduction is closely aligned with threat and vulnerability analyses and system archit	AC-6, CM-7, RA-3, SA-11.
SA-15(6)	Development Process, Standards, and Tools | Continuous Improvement	Require the developer of the system, system component, or system service to implement an explicit process to continuously improve the development process.	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.	None.
SA-15(7)	Development Process, Standards, and Tools | Automated Vulnerability Analysis	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].	Automated tools can be more effective at analyzing exploitable weaknesses or deficiencies in larg	RA-5, SA-11.
SA-15(8)	Development Process, Standards, and Tools | Reuse of Threat and Vulnerability Information	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.	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.	None.
SA-19(4)	Component Authenticity | Anti-counterfeit Scanning	[Withdrawn: Moved to SR-11(3).]		

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
SA-15(10)	Development Process, Standards, and Tools | Incident Response Plan	Require the developer of the system, system component, or system service to provide, implement	The incident response plan provided by developers may provide information not readily available	IR-8.
SA-15(11)	Development Process, Standards, and Tools | Archive System or Component	Require the developer of the system or system component to archive the system or component to	Archiving system or system components requires the developer to retain key development artifac	CM-2.
SA-15(12)	Development Process, Standards, and Tools | Minimize Personally Identifiable Information	Require the developer of the system or system component to minimize the use of personally iden	Organizations can minimize the risk to an individual's privacy by using techniques such as de-ident	PM-25, SA-3, SA-8.
SA-16	Developer-provided Training	Require the developer of the system, system component, or system service to provide the followin	Developer-provided training applies to external and internal (in-house) developers. Training perso	AT-2, AT-3, PE-3, SA-4, SA-5.
SA-17	Developer Security and Privacy Architecture and Design	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.	Developer security and privacy architecture and design are directed at external developers, althou	PL-2, PL-8, PM-7, SA-3, SA-4, SA-8, SC-7.
SA-17(1)	Developer Security and Privacy Architecture and Design | Formal Policy Model	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.	Formal models describe specific behaviors or security and privacy policies using formal languages,	AC-3, AC-4, AC-25.
SA-17(2)	Developer Security and Privacy Architecture and Design | Security-relevant Components	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.	The security-relevant hardware, software, and firmware represent the portion of the system, com	AC-25, SA-5.
SA-17(3)	Developer Security and Privacy Architecture and Design | Formal Correspondence	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.	Correspondence is an important part of the assurance gained through modeling. It demonstrates	AC-3, AC-4, AC-25, SA-4, SA-5.
SA-17(4)	Developer Security and Privacy Architecture and Design | Informal Correspondence	Require the developer of the system, system component, or system service to: (a) Produce, as an integral part of the development process, an informal descriptive top-level specification that specifies the interfaces to security-relevant hardware, software, and firmware in terms of exceptions, error messages, and effects; (b) Show via [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.	Correspondence is an important part of the assurance gained through modeling. It demonstrates	AC-3, AC-4, AC-25, SA-4, SA-5.
SA-17(5)	Developer Security and Privacy Architecture and Design | Conceptually Simple Design	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.	The principle of reduced complexity states that the system design is as simple and small as possibl	AC-25, SA-8, SC-3.
SA-17(6)	Developer Security and Privacy Architecture and Design | Structure for Testing	Require the developer of the system, system component, or system service to structure security-re	Applying the security design principles in SP 800-160-1 promotes complete, consistent, and compr	SA-5, SA-11.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
SA-17(7)	Developer Security and Privacy Architecture and Design | Structure for Least Privilege	Require the developer of the system, system component, or system service to structure security-re	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.	AC-5, AC-6, SA-8.
SA-17(8)	Developer Security and Privacy Architecture and Design | Orchestration	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].	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.	None.
SA-17(9)	Developer Security and Privacy Architecture and Design | Design Diversity	Use different designs for [Assignment: organization-defined critical systems or system components] to satisfy a common set of requirements or to provide equivalent functionality.	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.	None.
SA-21(1)	Developer Screening | Validation of Screening	[Withdrawn: Incorporated into SA-21.]		
SA-22(1)	Unsupported System Components | Alternative Sources for Continued Support	[Withdrawn: Incorporated into SA-22.]		
SA-4(4)	Acquisition Process | Assignment of Components to Systems	[Withdrawn: Incorporated into CM-8(9).]		
SA-5(1)	System Documentation | Functional Properties of Security Controls	[Withdrawn: Incorporated into SA-4(1).]		
SA-5(2)	System Documentation | Security-relevant External System Interfaces	[Withdrawn: Incorporated into SA-4(2).]		
SA-5(3)	System Documentation | High-level Design	[Withdrawn: Incorporated into SA-4(2).]		
SA-5(4)	System Documentation | Low-level Design	[Withdrawn: Incorporated into SA-4(2).]		
SA-5(5)	System Documentation | Source Code	[Withdrawn: Incorporated into SA-4(2).]		
SA-20	Customized Development of Critical Components	Reimplement or custom develop the following critical system components: [Assignment: organizat	Organizations determine that certain system components likely cannot be trusted due to specific t	CP-2, RA-9, SA-8.
SA-21	Developer Screening	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].	Developer screening is directed at external developers. Internal developer screening is addressed	PS-2, PS-3, PS-6, PS-7, SA-4, SR-6.
SA-6	Software Usage Restrictions	[Withdrawn: Incorporated into CM-10 and SI-7.]		

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
SA-22	Unsupported System Components	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]].	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.	PL-2, SA-3.
SA-7	User-installed Software	[Withdrawn: Incorporated into CM-11 and SI-7.]		
SA-23	Specialization	Employ [Selection (one or more): design; modification; augmentation; reconfiguration] on [Assign	It is often necessary for a system or system component that supports mission-essential services o	RA-9, SA-8.
SC-1	Policy and Procedures	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].	System and communications protection policy and procedures address the controls in the SC fami	PM-9, PS-8, SA-8, SI-12.
SC-2	Separation of System and User Functionality	Separate user functionality, including user interface services, from system management functiona	System management functionality includes functions that are necessary to administer databases,	AC-6, SA-4, SA-8, SC-3, SC-7, SC-22, SC-32, SC-39.
SC-2(1)	Separation of System and User Functionality | Interfaces for Non-privileged Users	Prevent the presentation of system management functionality at interfaces to non-privileged user	Preventing the presentation of system management functionality at interfaces to non-privileged u	AC-3.
SC-2(2)	Separation of System and User Functionality | Disassociability	Store state information from applications and software separately.	If a system is compromised, storing applications and software separately from state information about users' interactions with an application may better protect individuals' privacy.	None.
SC-3	Security Function Isolation	Isolate security functions from nonsecurity functions.	Security functions are isolated from nonsecurity functions by means of an isolation boundary imp	AC-3, AC-6, AC-25, CM-2, CM-4, SA-4, SA-5, SA-8, SA-15, SA-17, SC-2, SC-7, SC-32, SC-39, SI-16.
SC-3(1)	Security Function Isolation | Hardware Separation	Employ hardware separation mechanisms to implement security function isolation.	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).	None.
SC-3(2)	Security Function Isolation | Access and Flow Control Functions	Isolate security functions enforcing access and information flow control from nonsecurity functions and from other security functions.	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.	None.
SC-3(3)	Security Function Isolation | Minimize Nonsecurity Functionality	Minimize the number of nonsecurity functions included within the isolation boundary containing security functions.	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.	None.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
SC-3(4)	Security Function Isolation | Module Coupling and Cohesiveness	Implement security functions as largely independent modules that maximize internal cohesiveness within modules and minimize coupling between modules.	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.	None.
SC-3(5)	Security Function Isolation | Layered Structures	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.	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.	None.
SC-4	Information in Shared System Resources	Prevent unauthorized and unintended information transfer via shared system resources.	Preventing unauthorized and unintended information transfer via shared system resources stops	AC-3, AC-4, SA-8.
SC-12(4)	Cryptographic Key Establishment and Management | PKI Certificates	[Withdrawn: Incorporated into SC-12(3).]		
SC-4(2)	Information in Shared System Resources | Multilevel or Periods Processing	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.	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.	None.
SC-5	Denial-of-service Protection	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].	Denial-of-service events may occur due to a variety of internal and external causes, such as an att	CP-2, IR-4, SC-6, SC-7, SC-40.
SC-5(1)	Denial-of-service Protection | Restrict Ability to Attack Other Systems	Restrict the ability of individuals to launch the following denial-of-service attacks against other systems: [Assignment: organization-defined denial-of-service attacks].	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.	None.
SC-5(2)	Denial-of-service Protection | Capacity, Bandwidth, and Redundancy	Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding denial-of-service attacks.	Managing capacity ensures that sufficient capacity is available to counter flooding attacks. Managing capacity includes establishing selected usage priorities, quotas, partitioning, or load balancing.	None.
SC-5(3)	Denial-of-service Protection | Detection and Monitoring	(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].	Organizations consider the utilization and capacity of system resources when managing risk assoc	CA-7, SI-4.
SC-6	Resource Availability	Protect the availability of resources by allocating [Assignment: organization-defined resources] by	Priority protection prevents lower-priority processes from delaying or interfering with the system	SC-5.
SC-7	Boundary Protection	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.	Managed interfaces include gateways, routers, firewalls, guards, network-based malicious code ar	AC-4, AC-17, AC-18, AC-19, AC-20, AU-13, CA-3, CM-2, CM-4, CM-7, CM-10, CP-8, CP-10, IR-4, MA-4, PE-3, PL-8, PM-12, SA-8, SA-17, SC-5, SC-26, SC-32, SC-35, SC-43.
SC-12(5)	Cryptographic Key Establishment and Management | PKI Certificates / Hardware Tokens	[Withdrawn: Incorporated into SC-12(3).]		
SC-13(1)	Cryptographic Protection | FIPS-validated Cryptography	[Withdrawn: Incorporated into SC-13.]		
SC-7(3)	Boundary Protection | Access Points	Limit the number of external network connections to the system.	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.	None.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
SC-7(4)	Boundary Protection | External Telecommunications Services	(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.	External telecommunications services can provide data and/or voice communications services. Exa	AC-3, SC-8, SC-20, SC-21, SC-22.
SC-7(5)	Boundary Protection | Deny by Default — Allow by Exception	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]].	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.	None.
SC-13(2)	Cryptographic Protection | NSA-approved Cryptography	[Withdrawn: Incorporated into SC-13.]		
SC-7(7)	Boundary Protection | Split Tunneling for Remote Devices	Prevent split tunneling for remote devices connecting to organizational systems unless the split tunnel is securely provisioned using [Assignment: organization-defined safeguards].	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.	None.
SC-7(8)	Boundary Protection | Route Traffic to Authenticated Proxy Servers	Route [Assignment: organization-defined internal communications traffic] to [Assignment: organiz	External networks are networks outside of organizational control. A proxy server is a server (i.e., s	AC-3.
SC-7(9)	Boundary Protection | Restrict Threatening Outgoing Communications Traffic	(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.	Detecting outgoing communications traffic from internal actions that may pose threats to external	AU-2, AU-6, SC-5, SC-38, SC-44, SI-3, SI-4.
SC-7(10)	Boundary Protection | Prevent Exfiltration	(a) Prevent the exfiltration of information; and (b) Conduct exfiltration tests [Assignment: organization-defined frequency].	Prevention of exfiltration applies to both the intentional and unintentional exfiltration of informat	AC-2, CA-8, SI-3.
SC-7(11)	Boundary Protection | Restrict Incoming Communications Traffic	Only allow incoming communications from [Assignment: organization-defined authorized sources	General source address validation techniques are applied to restrict the use of illegal and unalloca	AC-3.
SC-7(12)	Boundary Protection | Host-based Protection	Implement [Assignment: organization-defined host-based boundary protection mechanisms] at [Assignment: organization-defined system components].	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.	None.
SC-7(13)	Boundary Protection | Isolation of Security Tools, Mechanisms, and Support Components	Isolate [Assignment: organization-defined information security tools, mechanisms, and support co	Physically separate subnetworks with managed interfaces are useful in isolating computer networ	SC-2, SC-3.
SC-7(14)	Boundary Protection | Protect Against Unauthorized Physical Connections	Protect against unauthorized physical connections at [Assignment: organization-defined managed	Systems that operate at different security categories or classification levels may share common ph	PE-4, PE-19.
SC-7(15)	Boundary Protection | Networked Privileged Accesses	Route networked, privileged accesses through a dedicated, managed interface for purposes of acc	Privileged access provides greater accessibility to system functions, including security functions. Ad	AC-2, AC-3, AU-2, SI-4.
SC-7(16)	Boundary Protection | Prevent Discovery of System Components	Prevent the discovery of specific system components that represent a managed interface.	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.	None.
SC-7(17)	Boundary Protection | Automated Enforcement of Protocol Formats	Enforce adherence to protocol formats.	System components that enforce protocol formats include deep packet inspection firewalls and X	SC-4.
SC-7(18)	Boundary Protection | Fail Secure	Prevent systems from entering unsecure states in the event of an operational failure of a boundar	Fail secure is a condition achieved by employing mechanisms to ensure that in the event of operat	CP-2, CP-12, SC-24.
SC-7(19)	Boundary Protection | Block Communication from Non-organizationally Configured Hosts	Block inbound and outbound communications traffic between [Assignment: organization-defined communication clients] that are independently configured by end users and external service providers.	Communication clients independently configured by end users and external service providers include instant messaging clients and video conferencing software and applications. Traffic blocking does not apply to communication clients that are configured by organizations to perform authorized functions.	None.
SC-7(20)	Boundary Protection | Dynamic Isolation and Segregation	Provide the capability to dynamically isolate [Assignment: organization-defined system components] from other system components.	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.	None.
SC-7(21)	Boundary Protection | Isolation of System Components	Employ boundary protection mechanisms to isolate [Assignment: organization-defined system co	Organizations can isolate system components that perform different mission or business function	CA-9.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
SC-7(22)	Boundary Protection | Separate Subnets for Connecting to Different Security Domains	Implement separate network addresses to connect to systems in different security domains.	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.	None.
SC-7(23)	Boundary Protection | Disable Sender Feedback on Protocol Validation Failure	Disable feedback to senders on protocol format validation failure.	Disabling feedback to senders when there is a failure in protocol validation format prevents adversaries from obtaining information that would otherwise be unavailable.	None.
SC-7(24)	Boundary Protection | Personally Identifiable Information	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.	Managing the processing of personally identifiable information is an important aspect of protectin	PT-2, SI-15.
SC-7(25)	Boundary Protection | Unclassified National Security System Connections	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].	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.	None.
SC-7(26)	Boundary Protection | Classified National Security System Connections	Prohibit the direct connection of a classified national security system to an external network without the use of [Assignment: organization-defined boundary protection device].	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.	None.
SC-7(27)	Boundary Protection | Unclassified Non-national Security System Connections	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].	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.	None.
SC-7(28)	Boundary Protection | Connections to Public Networks	Prohibit the direct connection of [Assignment: organization-defined system] to a public network.	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.	None.
SC-7(29)	Boundary Protection | Separate Subnets to Isolate Functions	Implement [Selection: physically; logically] separate subnetworks to isolate the following critical system components and functions: [Assignment: organization-defined critical system components and functions].	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.	None.
SC-8	Transmission Confidentiality and Integrity	Protect the [Selection (one or more): confidentiality; integrity] of transmitted information.	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.	AC-17, AC-18, AU-10, IA-3, IA-8, IA-9, MA-4, PE-4, SA-4, SA-8, SC-7, SC-16, SC-20, SC-23, SC-28.
SC-8(1)	Transmission Confidentiality and Integrity | Cryptographic Protection	Implement cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosu	Encryption protects information from unauthorized disclosure and modification during transmissi	SC-12, SC-13.
SC-8(2)	Transmission Confidentiality and Integrity | Pre- and Post-transmission Handling	Maintain the [Selection (one or more): confidentiality; integrity] of information during preparation for transmission and during reception.	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.	None.
SC-8(3)	Transmission Confidentiality and Integrity | Cryptographic Protection for Message Externals	Implement cryptographic mechanisms to protect message externals unless otherwise protected b	Cryptographic protection for message externals addresses protection from the unauthorized discl	SC-12, SC-13.
SC-8(4)	Transmission Confidentiality and Integrity | Conceal or Randomize Communications	Implement cryptographic mechanisms to conceal or randomize communication patterns unless ot	Concealing or randomizing communication patterns addresses protection from unauthorized disc	SC-12, SC-13.
SC-8(5)	Transmission Confidentiality and Integrity | Protected Distribution System	Implement [Assignment: organization-defined protected distribution system] to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.	The purpose of a protected distribution system is to deter, detect, and/or make difficult physical access to the communication lines that carry national security information.	None.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
SC-13(3)	Cryptographic Protection | Individuals Without Formal Access Approvals	[Withdrawn: Incorporated into SC-13.]		
SC-10	Network Disconnect	Terminate the network connection associated with a communications session at the end of the se	Network disconnect applies to internal and external networks. Terminating network connections a	AC-17, SC-23.
SC-11	Trusted Path	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].	Trusted paths are mechanisms by which users can communicate (using input devices such as keyb	AC-16, AC-25, SC-12, SC-23.
SC-11(1)	Trusted Path | Irrefutable Communications Path	(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.	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.	None.
SC-12	Cryptographic Key Establishment and Management	Establish and manage cryptographic keys when cryptography is employed within the system in acc	Cryptographic key management and establishment can be performed using manual procedures o	AC-17, AU-9, AU-10, CM-3, IA-3, IA-7, SA-4, SA-8, SA-9, SC-8, SC-11, SC-12, SC-13, SC-17, SC-20, SC-37, SC-40, SI-3, SI-7.
SC-12(1)	Cryptographic Key Establishment and Management | Availability	Maintain availability of information in the event of the loss of cryptographic keys by users.	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.	None.
SC-12(2)	Cryptographic Key Establishment and Management | Symmetric Keys	Produce, control, and distribute symmetric cryptographic keys using [Selection: NIST FIPS-validated; NSA-approved] key management technology and processes.	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.	None.
SC-12(3)	Cryptographic Key Establishment and Management | Asymmetric Keys	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].	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.	None.
SC-13(4)	Cryptographic Protection | Digital Signatures	[Withdrawn: Incorporated into SC-13.]		
SC-14	Public Access Protections	[Withdrawn: Incorporated into AC-2, AC-3, AC-5, AC-6, SI-3, SI-4, SI-5, SI-7, and SI-10.]		
SC-12(6)	Cryptographic Key Establishment and Management | Physical Control of Keys	Maintain physical control of cryptographic keys when stored information is encrypted by external service providers.	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.	None.
SC-13	Cryptographic Protection	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].	Cryptography can be employed to support a variety of security solutions, including the protection	AC-2, AC-3, AC-7, AC-17, AC-18, AC-19, AU-9, AU-10, CM-11, CP-9, IA-3, IA-5, IA-7, MA-4, MP-2, MP-4, MP-5, SA-4, SA-8, SA-9, SC-8, SC-12, SC-20, SC-23, SC-28, SC-40, SI-3, SI-7.
SC-15(2)	Collaborative Computing Devices and Applications | Blocking Inbound and Outbound Communications Traffic	[Withdrawn: Incorporated into SC-7.]		
SC-19	Voice Over Internet Protocol	[Withdrawn: Technology-specific; addressed as any other technology or protocol.]		
SC-20(1)	Secure Name/address Resolution Service (authoritative Source) | Child Subspaces	[Withdrawn: Incorporated into SC-20.]		
SC-21(1)	Secure Name/address Resolution Service (recursive or Caching Resolver) | Data Origin and Integrity	[Withdrawn: Incorporated into SC-21.]		
SC-23(2)	Session Authenticity | User-initiated Logouts and Message Displays	[Withdrawn: Incorporated into AC-12(1).]		
SC-15	Collaborative Computing Devices and Applications	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.	Collaborative computing devices and applications include remote meeting devices and application	AC-21, SC-42.
SC-15(1)	Collaborative Computing Devices and Applications | Physical or Logical Disconnect	Provide [Selection (one or more): physical; logical] disconnect of collaborative computing devices in a manner that supports ease of use.	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.	None.
SC-23(4)	Session Authenticity | Unique Session Identifiers with Randomization	[Withdrawn: Incorporated into SC-23(3).]		
SC-15(3)	Collaborative Computing Devices and Applications | Disabling and Removal in Secure Work Areas	Disable or remove collaborative computing devices and applications from [Assignment: organization-defined systems or system components] in [Assignment: organization-defined secure work areas].	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.	None.
SC-15(4)	Collaborative Computing Devices and Applications | Explicitly Indicate Current Participants	Provide an explicit indication of current participants in [Assignment: organization-defined online meetings and teleconferences].	Explicitly indicating current participants prevents unauthorized individuals from participating in collaborative computing sessions without the explicit knowledge of other participants.	None.
SC-16	Transmission of Security and Privacy Attributes	Associate [Assignment: organization-defined security and privacy attributes] with information exc	Security and privacy attributes can be explicitly or implicitly associated with the information contai	AC-3, AC-4, AC-16.
SC-16(1)	Transmission of Security and Privacy Attributes | Integrity Verification	Verify the integrity of transmitted security and privacy attributes.	Part of verifying the integrity of transmitted information is ensuring that security and privacy attrib	AU-10, SC-8.
SC-16(2)	Transmission of Security and Privacy Attributes | Anti-spoofing Mechanisms	Implement anti-spoofing mechanisms to prevent adversaries from falsifying the security attributes	Some attack vectors operate by altering the security attributes of an information system to intenti	SI-3, SI-4, SI-7.
SC-16(3)	Transmission of Security and Privacy Attributes | Cryptographic Binding	Implement [Assignment: organization-defined mechanisms or techniques] to bind security and pri	Cryptographic mechanisms and techniques can provide strong security and privacy attribute bindi	AC-16, SC-12, SC-13.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
SC-17	Public Key Infrastructure Certificates	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.	Public key infrastructure (PKI) certificates are certificates with visibility external to organizational s	AU-10, IA-5, SC-12.
SC-18	Mobile Code	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.	Mobile code includes any program, application, or content that can be transmitted across a netwo	AU-2, AU-12, CM-2, CM-6, SI-3.
SC-18(1)	Mobile Code | Identify Unacceptable Code and Take Corrective Actions	Identify [Assignment: organization-defined unacceptable mobile code] and take [Assignment: organization-defined corrective actions].	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.	None.
SC-18(2)	Mobile Code | Acquisition, Development, and Use	Verify that the acquisition, development, and use of mobile code to be deployed in the system meets [Assignment: organization-defined mobile code requirements].	None.	None.
SC-18(3)	Mobile Code | Prevent Downloading and Execution	Prevent the download and execution of [Assignment: organization-defined unacceptable mobile code].	None.	None.
SC-18(4)	Mobile Code | Prevent Automatic Execution	Prevent the automatic execution of mobile code in [Assignment: organization-defined software applications] and enforce [Assignment: organization-defined actions] prior to executing the code.	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.	None.
SC-18(5)	Mobile Code | Allow Execution Only in Confined Environments	Allow execution of permitted mobile code only in confined virtual machine environments.	Permitting the execution of mobile code only in confined virtual machine environments helps prev	SC-44, SI-7.
SC-26(1)	Decoys | Detection of Malicious Code	[Withdrawn: Incorporated into SC-35.]		
SC-20	Secure Name/address Resolution Service (authoritative Source)	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.	Providing authoritative source information enables external clients, including remote Internet clie	AU-10, SC-8, SC-12, SC-13, SC-21, SC-22.
SC-30(1)	Concealment and Misdirection | Virtualization Techniques	[Withdrawn: Incorporated into SC-29(1).]		
SC-20(2)	Secure Name/address Resolution Service (authoritative Source) | Data Origin and Integrity	Provide data origin and integrity protection artifacts for internal name/address resolution queries.	None.	None.
SC-21	Secure Name/address Resolution Service (recursive or Caching Resolver)	Request and perform data origin authentication and data integrity verification on the name/addre	Each client of name resolution services either performs this validation on its own or has authentic	SC-20, SC-22.
SC-33	Transmission Preparation Integrity	[Withdrawn: Incorporated into SC-8.]		
SC-22	Architecture and Provisioning for Name/address Resolution Service	Ensure the systems that collectively provide name/address resolution service for an organization a	Systems that provide name and address resolution services include domain name system (DNS) se	SC-2, SC-20, SC-21, SC-24.
SC-23	Session Authenticity	Protect the authenticity of communications sessions.	Protecting session authenticity addresses communications protection at the session level, not at th	AU-10, SC-8, SC-10, SC-11.
SC-23(1)	Session Authenticity | Invalidate Session Identifiers at Logout	Invalidate session identifiers upon user logout or other session termination.	Invalidating session identifiers at logout curtails the ability of adversaries to capture and continue to employ previously valid session IDs.	None.
SC-34(3)	Non-modifiable Executable Programs | Hardware-based Protection	[Withdrawn: Moved to SC-51.]		
SC-23(3)	Session Authenticity | Unique System-generated Session Identifiers	Generate a unique session identifier for each session with [Assignment: organization-defined rand	Generating unique session identifiers curtails the ability of adversaries to reuse previously valid se	AC-10, SC-12, SC-13.
SC-4(1)	Information in Shared System Resources | Security Levels	[Withdrawn: Incorporated into SC-4.]		
SC-23(5)	Session Authenticity | Allowed Certificate Authorities	Only allow the use of [Assignment: organization-defined certificate authorities] for verification of t	Reliance on certificate authorities for the establishment of secure sessions includes the use of Tra	SC-12, SC-13.
SC-24	Fail in Known State	Fail to a [Assignment: organization-defined known system state] for the following failures on the i	Failure in a known state addresses security concerns in accordance with the mission and business	CP-2, CP-4, CP-10, CP-12, SA-8, SC-7, SC-22, SI-13.
SC-25	Thin Nodes	Employ minimal functionality and information storage on the following system components: [Assi	The deployment of system components with minimal functionality reduces the need to secure eve	SC-30, SC-44.
SC-26	Decoys	Include components within organizational systems specifically designed to be the target of malicio	Decoys (i.e., honeypots, honeynets, or deception nets) are established to attract adversaries and d	RA-5, SC-7, SC-30, SC-35, SC-44, SI-3, SI-4.
SC-42(3)	Sensor Capability and Data | Prohibit Use of Devices	[Withdrawn: Incorporated into SC-42.]		
SC-27	Platform-independent Applications	Include within organizational systems the following platform independent applications: [Assignme	Platforms are combinations of hardware, firmware, and software components used to execute so	SC-29.
SC-28	Protection of Information at Rest	Protect the [Selection (one or more): confidentiality; integrity] of the following information at rest:	Information at rest refers to the state of information when it is not in process or in transit and is lo	AC-3, AC-4, AC-6, AC-19, CA-7, CM-3, CM-5, CM-6, CP-9, MP-4, MP-5, PE-3, SC-8, SC-12, SC-13, SC-34, SI-3, SI-7, SI-16.
SC-28(1)	Protection of Information at Rest | Cryptographic Protection	Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the	The selection of cryptographic mechanisms is based on the need to protect the confidentiality and	AC-19, SC-12, SC-13.
SC-28(2)	Protection of Information at Rest | Offline Storage	Remove the following information from online storage and store offline in a secure location: [Assignment: organization-defined information].	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.	None.
SC-28(3)	Protection of Information at Rest | Cryptographic Keys	Provide protected storage for cryptographic keys [Selection: [Assignment: organization-defined sa	A Trusted Platform Module (TPM) is an example of a hardware-protected data store that can be u	SC-12, SC-13.
SC-29	Heterogeneity	Employ a diverse set of information technologies for the following system components in the impl	Increasing the diversity of information technologies within organizational systems reduces the imp	AU-9, PL-8, SC-27, SC-30, SR-3.
SC-29(1)	Heterogeneity | Virtualization Techniques	Employ virtualization techniques to support the deployment of a diversity of operating systems and applications that are changed [Assignment: organization-defined frequency].	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.	None.
SC-30	Concealment and Misdirection	Employ the following concealment and misdirection techniques for [Assignment: organization-def	Concealment and misdirection techniques can significantly reduce the targeting capabilities of adv	AC-6, SC-25, SC-26, SC-29, SC-44, SI-14.
SC-7(1)	Boundary Protection | Physically Separated Subnetworks	[Withdrawn: Incorporated into SC-7.]		

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
SC-30(2)	Concealment and Misdirection | Randomness	Employ [Assignment: organization-defined techniques] to introduce randomness into organizational operations and assets.	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.	None.
SC-30(3)	Concealment and Misdirection | Change Processing and Storage Locations	Change the location of [Assignment: organization-defined processing and/or storage] [Selection: [Assignment: organization-defined time frequency]; at random time intervals]].	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.	None.
SC-30(4)	Concealment and Misdirection | Misleading Information	Employ realistic, but misleading information in [Assignment: organization-defined system components] about its security state or posture.	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.	None.
SC-30(5)	Concealment and Misdirection | Concealment of System Components	Employ the following techniques to hide or conceal [Assignment: organization-defined system components]: [Assignment: organization-defined techniques].	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.	None.
SC-31	Covert Channel Analysis	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.	Developers are in the best position to identify potential areas within systems that might lead to co	AC-3, AC-4, SA-8, SI-11.
SC-31(1)	Covert Channel Analysis | Test Covert Channels for Exploitability	Test a subset of the identified covert channels to determine the channels that are exploitable.	None.	None.
SC-31(2)	Covert Channel Analysis | Maximum Bandwidth	Reduce the maximum bandwidth for identified covert [Selection (one or more): storage; timing] channels to [Assignment: organization-defined values].	The complete elimination of covert channels, especially covert timing channels, is usually not possible without significant performance impacts.	None.
SC-31(3)	Covert Channel Analysis | Measure Bandwidth in Operational Environments	Measure the bandwidth of [Assignment: organization-defined subset of identified covert channels] in the operational environment of the system.	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.	None.
SC-32	System Partitioning	Partition the system into [Assignment: organization-defined system components] residing in separ	System partitioning is part of a defense-in-depth protection strategy. Organizations determine the	AC-4, AC-6, SA-8, SC-2, SC-3, SC-7, SC-36.
SC-32(1)	System Partitioning | Separate Physical Domains for Privileged Functions	Partition privileged functions into separate physical domains.	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.	None.
SC-7(2)	Boundary Protection | Public Access	[Withdrawn: Incorporated into SC-7.]		
SC-34	Non-modifiable Executable Programs	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].	The operating environment for a system contains the code that hosts applications, including opera	AC-3, SI-7, SI-14.
SC-34(1)	Non-modifiable Executable Programs | No Writable Storage	Employ [Assignment: organization-defined system components] with no writeable storage that is	Disallowing writeable storage eliminates the possibility of malicious code insertion via persistent,	AC-19, MP-7.
SC-34(2)	Non-modifiable Executable Programs | Integrity Protection on Read-only Media	Protect the integrity of information prior to storage on read-only media and control the media aft	Controls prevent the substitution of media into systems or the reprogramming of programmable	CM-3, CM-5, CM-9, MP-2, MP-4, MP-5, SC-28, SI-3.
SC-7(6)	Boundary Protection | Response to Recognized Failures	[Withdrawn: Incorporated into SC-7(18).]		
SC-35	External Malicious Code Identification	Include system components that proactively seek to identify network-based malicious code or ma	External malicious code identification differs from decoys in SC-26 in that the components actively	SC-7, SC-26, SC-44, SI-3, SI-4.
SC-36	Distributed Processing and Storage	Distribute the following processing and storage components across multiple [Selection: physical lo	Distributing processing and storage across multiple physical locations or logical domains provides	CP-6, CP-7, PL-8, SC-32.
SC-36(1)	Distributed Processing and Storage | Polling Techniques	(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].	Distributed processing and/or storage may be used to reduce opportunities for adversaries to con	SI-4.
SC-36(2)	Distributed Processing and Storage | Synchronization	Synchronize the following duplicate systems or system components: [Assignment: organization-de	SC-36 and CP-9(6) require the duplication of systems or system components in distributed locatio	CP-9.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
SC-37	Out-of-band Channels	Employ the following out-of-band channels for the physical delivery or electronic transmission of [	Out-of-band channels include local, non-network accesses to systems; network paths physically se	AC-2, CM-3, CM-5, CM-7, IA-2, IA-4, IA-5, MA-4, SC-12, SI-3, SI-4, SI-7.
SC-37(1)	Out-of-band Channels | Ensure Delivery and Transmission	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].	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.	None.
SC-38	Operations Security	Employ the following operations security controls to protect key organizational information throu	Operations security (OPSEC) is a systematic process by which potential adversaries can be denied	CA-2, CA-7, PL-1, PM-9, PM-12, RA-2, RA-3, RA-5, SC-7, SR-3, SR-7.
SC-39	Process Isolation	Maintain a separate execution domain for each executing system process.	Systems can maintain separate execution domains for each executing process by assigning each p	AC-3, AC-4, AC-6, AC-25, SA-8, SC-2, SC-3, SI-16.
SC-39(1)	Process Isolation | Hardware Separation	Implement hardware separation mechanisms to facilitate process isolation.	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.	None.
SC-39(2)	Process Isolation | Separate Execution Domain Per Thread	Maintain a separate execution domain for each thread in [Assignment: organization-defined multi-threaded processing].	None.	None.
SC-40	Wireless Link Protection	Protect external and internal [Assignment: organization-defined wireless links] from the following	Wireless link protection applies to internal and external wireless communication links that may be	AC-18, SC-5.
SC-40(1)	Wireless Link Protection | Electromagnetic Interference	Implement cryptographic mechanisms that achieve [Assignment: organization-defined level of pro	The implementation of cryptographic mechanisms for electromagnetic interference protects syste	PE-21, SC-12, SC-13.
SC-40(2)	Wireless Link Protection | Reduce Detection Potential	Implement cryptographic mechanisms to reduce the detection potential of wireless links to [Assig	The implementation of cryptographic mechanisms to reduce detection potential is used for covert	SC-12, SC-13.
SC-40(3)	Wireless Link Protection | Imitative or Manipulative Communications Deception	Implement cryptographic mechanisms to identify and reject wireless transmissions that are delibe	The implementation of cryptographic mechanisms to identify and reject imitative or manipulative	SC-12, SC-13, SI-4.
SC-40(4)	Wireless Link Protection | Signal Parameter Identification	Implement cryptographic mechanisms to prevent the identification of [Assignment: organization-d	The implementation of cryptographic mechanisms to prevent the identification of wireless transm	SC-12, SC-13.
SC-41	Port and I/O Device Access	[Selection: Physically; Logically] disable or remove [Assignment: organization-defined connection p	Connection ports include Universal Serial Bus (USB), Thunderbolt, and Firewire (IEEE 1394). Input/	AC-20, MP-7.
SC-42	Sensor Capability and Data	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].	Sensor capability and data applies to types of systems or system components characterized as mo	SC-15.
SC-42(1)	Sensor Capability and Data | Reporting to Authorized Individuals or Roles	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.	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.	None.
SC-42(2)	Sensor Capability and Data | Authorized Use	Employ the following measures so that data or information collected by [Assignment: organization	Information collected by sensors for a specific authorized purpose could be misused for some una	PT-2.
SC-9	Transmission Confidentiality	[Withdrawn: Incorporated into SC-8.]		
SC-42(4)	Sensor Capability and Data | Notice of Collection	Employ the following measures to facilitate an individual's awareness that personally identifiable	Awareness that organizational sensors are collecting data enables individuals to more effectively e	PT-1, PT-4, PT-5.
SC-42(5)	Sensor Capability and Data | Collection Minimization	Employ [Assignment: organization-defined sensors] that are configured to minimize the collection	Although policies to control for authorized use can be applied to information once it is collected, n	SA-8, SI-12.
SC-43	Usage Restrictions	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.	Usage restrictions apply to all system components including but not limited to mobile code, mobile	AC-18, AC-19, CM-6, SC-7, SC-18.
SC-44	Detonation Chambers	Employ a detonation chamber capability within [Assignment: organization-defined system, system	Detonation chambers, also known as dynamic execution environments, allow organizations to ope	SC-7, SC-18, SC-25, SC-26, SC-30, SC-35, SC-39, SI-3, SI-7.
SC-45	System Time Synchronization	Synchronize system clocks within and between systems and system components.	Time synchronization of system clocks is essential for the correct execution of many system servic	AC-3, AU-8, IA-2, IA-8.
SC-45(1)	System Time Synchronization | Synchronization with Authoritative Time Source	(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].	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.	None.
SC-45(2)	System Time Synchronization | Secondary Authoritative Time Source	(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.	It may be necessary to employ geolocation information to determine that the secondary authoritative time source is in a different geographic region.	None.
SC-46	Cross Domain Policy Enforcement	Implement a policy enforcement mechanism [Selection: physically; logically] between the physical	For logical policy enforcement mechanisms, organizations avoid creating a logical path between in	AC-4, SC-7.
SC-47	Alternate Communications Paths	Establish [Assignment: organization-defined alternate communications paths] for system operatio	An incident, whether adversarial- or nonadversarial-based, can disrupt established communicatio	CP-2, CP-8.
SC-48	Sensor Relocation	Relocate [Assignment: organization-defined sensors and monitoring capabilities] to [Assignment: o	Adversaries may take various paths and use different approaches as they move laterally through a	AU-2, SC-7, SI-4.
SC-48(1)	Sensor Relocation | Dynamic Relocation of Sensors or Monitoring Capabilities	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].	None.	None.
SC-49	Hardware-enforced Separation and Policy Enforcement	Implement hardware-enforced separation and policy enforcement mechanisms between [Assignm	System owners may require additional strength of mechanism and robustness to ensure domain s	AC-4, SA-8, SC-50.
SC-50	Software-enforced Separation and Policy Enforcement	Implement software-enforced separation and policy enforcement mechanisms between [Assignm	System owners may require additional strength of mechanism to ensure domain separation and p	AC-3, AC-4, SA-8, SC-2, SC-3, SC-49.
SC-51	Hardware-based Protection	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.	None.	None.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
SI-1	Policy and Procedures	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].	System and information integrity policy and procedures address the controls in the SI family that a	PM-9, PS-8, SA-8, SI-12.
SI-2	Flaw Remediation	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.	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.	CA-5, CM-3, CM-4, CM-5, CM-6, CM-8, MA-2, RA-5, SA-8, SA-10, SA-11, SI-3, SI-5, SI-7, SI-11.
SI-13(2)	Predictable Failure Prevention | Time Limit on Process Execution Without Supervision	[Withdrawn: Incorporated into SI-7(16).]		
SI-2(2)	Flaw Remediation | Automated Flaw Remediation Status	Determine if system components have applicable security-relevant software and firmware update	Automated mechanisms can track and determine the status of known flaws for system componen	CA-7, SI-4.
SI-2(3)	Flaw Remediation | Time to Remediate Flaws and Benchmarks for Corrective Actions	(a) Measure the time between flaw identification and flaw remediation; and (b) Establish the following benchmarks for taking corrective actions: [Assignment: organization-defined benchmarks].	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.	None.
SI-2(4)	Flaw Remediation | Automated Patch Management Tools	Employ automated patch management tools to facilitate flaw remediation to the following system components: [Assignment: organization-defined system components].	Using automated tools to support patch management helps to ensure the timeliness and completeness of system patching operations.	None.
SI-2(5)	Flaw Remediation | Automatic Software and Firmware Updates	Install [Assignment: organization-defined security-relevant software and firmware updates] automatically to [Assignment: organization-defined system components].	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.	None.
SI-2(6)	Flaw Remediation | Removal of Previous Versions of Software and Firmware	Remove previous versions of [Assignment: organization-defined software and firmware components] after updated versions have been installed.	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.	None.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
SI-3	Malicious Code Protection	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.	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	AC-4, AC-19, CM-3, CM-8, IR-4, MA-3, MA-4, PL-9, RA-5, SC-7, SC-23, SC-26, SC-28, SC-44, SI-2, SI-4, SI-7, SI-8, SI-15.
SI-2(1)	Flaw Remediation | Central Management	[Withdrawn: Incorporated into PL-9.]		
SI-3(1)	Malicious Code Protection | Central Management	[Withdrawn: Incorporated into PL-9.]		
SI-3(2)	Malicious Code Protection | Automatic Updates	[Withdrawn: Incorporated into SI-3.]		
SI-3(4)	Malicious Code Protection | Updates Only by Privileged Users	Update malicious code protection mechanisms only when directed by a privileged user.	Protection mechanisms for malicious code are typically categorized as security-related software ar	CM-5.
SI-3(3)	Malicious Code Protection | Non-privileged Users	[Withdrawn: Incorporated into AC-6(10).]		
SI-3(6)	Malicious Code Protection | Testing and Verification	(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.	None.	CA-2, CA-7, RA-5.
SI-3(5)	Malicious Code Protection | Portable Storage Devices	[Withdrawn: Incorporated into MP-7.]		
SI-3(8)	Malicious Code Protection | Detect Unauthorized Commands	(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].	Detecting unauthorized commands can be applied to critical interfaces other than kernel-based in	AU-2, AU-6, AU-12.
SI-3(7)	Malicious Code Protection | Nonsignature-based Detection	[Withdrawn: Incorporated into SI-3.]		
SI-3(10)	Malicious Code Protection | Malicious Code Analysis	(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.	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.	None.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
SI-4	System Monitoring	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]].	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,	AC-2, AC-3, AC-4, AC-8, AC-17, AU-2, AU-6, AU-7, AU-9, AU-12, AU-13, AU-14, CA-7, CM-3, CM-6, CM-8, CM-11, IA-10, IR-4, MA-3, MA-4, PL-9, PM-12, RA-5, RA-10, SC-5, SC-7, SC-18, SC-26, SC-31, SC-35, SC-36, SC-37, SC-43, SI-3, SI-6, SI-7, SR-9, SR-10.
SI-4(1)	System Monitoring | System-wide Intrusion Detection System	Connect and configure individual intrusion detection tools into a system-wide intrusion detection system.	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.	None.
SI-4(2)	System Monitoring | Automated Tools and Mechanisms for Real-time Analysis	Employ automated tools and mechanisms to support near real-time analysis of events.	Automated tools and mechanisms include host-based, network-based, transport-based, or storag	PM-23, PM-25.
SI-4(3)	System Monitoring | Automated Tool and Mechanism Integration	Employ automated tools and mechanisms to integrate intrusion detection tools and mechanisms i	Using automated tools and mechanisms to integrate intrusion detection tools and mechanisms int	PM-23, PM-25.
SI-4(4)	System Monitoring | Inbound and Outbound Communications Traffic	(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].	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.	None.
SI-4(5)	System Monitoring | System-generated Alerts	Alert [Assignment: organization-defined personnel or roles] when the following system-generated	Alerts may be generated from a variety of sources, including audit records or inputs from maliciou	AU-4, AU-5, PE-6.
SI-3(9)	Malicious Code Protection | Authenticate Remote Commands	[Withdrawn: Moved to AC-17(10).]		
SI-4(7)	System Monitoring | Automated Response to Suspicious Events	(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].	Least-disruptive actions include initiating requests for human responses.	None.
SI-4(6)	System Monitoring | Restrict Non-privileged Users	[Withdrawn: Incorporated into AC-6(10).]		
SI-4(9)	System Monitoring | Testing of Monitoring Tools and Mechanisms	Test intrusion-monitoring tools and mechanisms [Assignment: organization-defined frequency].	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.	None.
SI-4(10)	System Monitoring | Visibility of Encrypted Communications	Make provisions so that [Assignment: organization-defined encrypted communications traffic] is visible to [Assignment: organization-defined system monitoring tools and mechanisms].	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.	None.
SI-4(11)	System Monitoring | Analyze Communications Traffic Anomalies	Analyze outbound communications traffic at the external interfaces to the system and selected [Assignment: organization-defined interior points within the system] to discover anomalies.	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.	None.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
SI-4(12)	System Monitoring | Automated Organization-generated Alerts	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].	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.	None.
SI-4(13)	System Monitoring | Analyze Traffic and Event Patterns	(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.	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.	None.
SI-4(14)	System Monitoring | Wireless Intrusion Detection	Employ a wireless intrusion detection system to identify rogue wireless devices and to detect attac	Wireless signals may radiate beyond organizational facilities. Organizations proactively search for	AC-18, IA-3.
SI-4(15)	System Monitoring | Wireless to Wireline Communications	Employ an intrusion detection system to monitor wireless communications traffic as the traffic pa	Wireless networks are inherently less secure than wired networks. For example, wireless network	AC-18.
SI-4(16)	System Monitoring | Correlate Monitoring Information	Correlate information from monitoring tools and mechanisms employed throughout the system.	Correlating information from different system monitoring tools and mechanisms can provide a m	AU-6.
SI-4(17)	System Monitoring | Integrated Situational Awareness	Correlate information from monitoring physical, cyber, and supply chain activities to achieve integ	Correlating monitoring information from a more diverse set of information sources helps to achie	AU-16, PE-6, SR-2, SR-4, SR-6.
SI-4(18)	System Monitoring | Analyze Traffic and Covert Exfiltration	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].	Organization-defined interior points include subnetworks and subsystems. Covert means that can be used to exfiltrate information include steganography.	None.
SI-4(19)	System Monitoring | Risk for Individuals	Implement [Assignment: organization-defined additional monitoring] of individuals who have been identified by [Assignment: organization-defined sources] as posing an increased level of risk.	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.	None.
SI-4(20)	System Monitoring | Privileged Users	Implement the following additional monitoring of privileged users: [Assignment: organization-defi	Privileged users have access to more sensitive information, including security-related information,	AC-18.
SI-4(21)	System Monitoring | Probationary Periods	Implement the following additional monitoring of individuals during [Assignment: organization-de	During probationary periods, employees do not have permanent employment status within organ	AC-18.
SI-4(22)	System Monitoring | Unauthorized Network Services	(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.	Unauthorized or unapproved network services include services in service-oriented architectures th	CM-7.
SI-4(23)	System Monitoring | Host-based Devices	Implement the following host-based monitoring mechanisms at [Assignment: organization-define	Host-based monitoring collects information about the host (or system in which it resides). System	AC-18, AC-19.
SI-4(24)	System Monitoring | Indicators of Compromise	Discover, collect, and distribute to [Assignment: organization-defined personnel or roles], indicato	Indicators of compromise (IOC) are forensic artifacts from intrusions that are identified on organi	AC-18.
SI-4(25)	System Monitoring | Optimize Network Traffic Analysis	Provide visibility into network traffic at external and key internal system interfaces to optimize the effectiveness of monitoring devices.	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.	None.
SI-5	Security Alerts, Advisories, and Directives	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.	The Cybersecurity and Infrastructure Security Agency (CISA) generates security alerts and advisori	PM-15, RA-5, SI-2.
SI-5(1)	Security Alerts, Advisories, and Directives | Automated Alerts and Advisories	Broadcast security alert and advisory information throughout the organization using [Assignment: organization-defined automated mechanisms].	The significant number of changes to organizational systems and environments of operation requires the dissemination of security-related information to a variety of organizational entities that have a direct 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.	None.
SI-6	Security and Privacy Function Verification	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.	Transitional states for systems include system startup, restart, shutdown, and abort. System notifi	CA-7, CM-4, CM-6, SI-7.
SI-4(8)	System Monitoring | Protection of Monitoring Information	[Withdrawn: Incorporated into SI-4.]		
SI-6(2)	Security and Privacy Function Verification | Automation Support for Distributed Testing	Implement automated mechanisms to support the management of distributed security and privac	The use of automated mechanisms to support the management of distributed function testing hel	SI-2.
SI-6(3)	Security and Privacy Function Verification | Report Verification Results	Report the results of security and privacy function verification to [Assignment: organization-define	Organizational personnel with potential interest in the results of the verification of security and pr	SI-4, SR-4, SR-5.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
SI-7	Software, Firmware, and Information Integrity	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].	Unauthorized changes to software, firmware, and information can occur due to errors or maliciou	AC-4, CM-3, CM-7, CM-8, MA-3, MA-4, RA-5, SA-8, SA-9, SA-10, SC-8, SC-12, SC-13, SC-28, SC-37, SI-3, SR-3, SR-4, SR-5, SR-6, SR-9, SR-10, SR-11.
SI-7(1)	Software, Firmware, and Information Integrity | Integrity Checks	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]].	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.	None.
SI-7(2)	Software, Firmware, and Information Integrity | Automated Notifications of Integrity Violations	Employ automated tools that provide notification to [Assignment: organization-defined personnel or roles] upon discovering discrepancies during integrity verification.	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.	None.
SI-7(3)	Software, Firmware, and Information Integrity | Centrally Managed Integrity Tools	Employ centrally managed integrity verification tools.	Centrally managed integrity verification tools provides greater consistency in the application of su	AU-3, SI-2, SI-8.
SI-6(1)	Security and Privacy Function Verification | Notification of Failed Security Tests	[Withdrawn: Incorporated into SI-6.]		
SI-7(5)	Software, Firmware, and Information Integrity | Automated Response to Integrity Violations	Automatically [Selection (one or more): shut the system down; restart the system; implement [Assignment: organization-defined controls]] when integrity violations are discovered.	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.	None.
SI-7(6)	Software, Firmware, and Information Integrity | Cryptographic Protection	Implement cryptographic mechanisms to detect unauthorized changes to software, firmware, and	Cryptographic mechanisms used to protect integrity include digital signatures and the computatio	SC-12, SC-13.
SI-7(7)	Software, Firmware, and Information Integrity | Integration of Detection and Response	Incorporate the detection of the following unauthorized changes into the organizational incident r	Integrating detection and response helps to ensure that detected events are tracked, monitored, c	AU-2, AU-6, IR-4, IR-5, SI-4.
SI-7(8)	Software, Firmware, and Information Integrity | Auditing Capability for Significant Events	Upon detection of a potential integrity violation, provide the capability to audit the event and initi	Organizations select response actions based on types of software, specific software, or informatio	AU-2, AU-6, AU-12.
SI-7(9)	Software, Firmware, and Information Integrity | Verify Boot Process	Verify the integrity of the boot process of the following system components: [Assignment: organiz	Ensuring the integrity of boot processes is critical to starting system components in known, trustw	SI-6.
SI-7(10)	Software, Firmware, and Information Integrity | Protection of Boot Firmware	Implement the following mechanisms to protect the integrity of boot firmware in [Assignment: org	Unauthorized modifications to boot firmware may indicate a sophisticated, targeted attack. These	SI-6.
SI-7(11)	Software, Firmware, and Information Integrity | Confined Environments with Limited Privileges	[Withdrawn: Moved to CM-7(6).]		
SI-7(12)	Software, Firmware, and Information Integrity | Integrity Verification	Require that the integrity of the following user-installed software be verified prior to execution: [A	Organizations verify the integrity of user-installed software prior to execution to reduce the likelih	CM-11.
SI-7(13)	Software, Firmware, and Information Integrity | Code Execution in Protected Environments	[Withdrawn: Moved to CM-7(7).]		
SI-7(14)	Software, Firmware, and Information Integrity | Binary or Machine Executable Code	[Withdrawn: Moved to CM-7(8).]		
SI-7(15)	Software, Firmware, and Information Integrity | Code Authentication	Implement cryptographic mechanisms to authenticate the following software or firmware compo	Cryptographic authentication includes verifying that software or firmware components have been	CM-5, SC-12, SC-13.
SI-7(16)	Software, Firmware, and Information Integrity | Time Limit on Process Execution Without Supervision	Prohibit processes from executing without supervision for more than [Assignment: organization-defined time period].	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.	None.
SI-7(17)	Software, Firmware, and Information Integrity | Runtime Application Self-protection	Implement [Assignment: organization-defined controls] for application self-protection at runtime.	Runtime application self-protection employs runtime instrumentation to detect and block the exp	SI-16.
SI-8	Spam Protection	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.	System entry and exit points include firewalls, remote-access servers, electronic mail servers, web	PL-9, SC-5, SC-7, SC-38, SI-3, SI-4.
SI-7(4)	Software, Firmware, and Information Integrity | Tamper-evident Packaging	[Withdrawn: Incorporated into SR-9.]		
SI-8(2)	Spam Protection | Automatic Updates	Automatically update spam protection mechanisms [Assignment: organization-defined frequency].	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.	None.
SI-8(3)	Spam Protection | Continuous Learning Capability	Implement spam protection mechanisms with a learning capability to more effectively identify legitimate communications traffic.	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.	None.
SI-8(1)	Spam Protection | Central Management	[Withdrawn: Incorporated into PL-9.]		

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
SI-10	Information Input Validation	Check the validity of the following information inputs: [Assignment: organization-defined information inputs to the system].	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.	None.
SI-10(1)	Information Input Validation | Manual Override Capability	(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.	In certain situations, such as during events that are defined in contingency plans, a manual overrid	AC-3, AU-2, AU-12.
SI-10(2)	Information Input Validation | Review and Resolve Errors	Review and resolve input validation errors within [Assignment: organization-defined time period].	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).	None.
SI-10(3)	Information Input Validation | Predictable Behavior	Verify that the system behaves in a predictable and documented manner when invalid inputs are received.	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).	None.
SI-10(4)	Information Input Validation | Timing Interactions	Account for timing interactions among system components in determining appropriate responses for invalid inputs.	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).	None.
SI-10(5)	Information Input Validation | Restrict Inputs to Trusted Sources and Approved Formats	Restrict the use of information inputs to [Assignment: organization-defined trusted sources] and/	Restricting the use of inputs to trusted sources and in trusted formats applies the concept of auth	AC-3, AC-6.
SI-10(6)	Information Input Validation | Injection Prevention	Prevent untrusted data injections.	Untrusted data injections may be prevented using a parameterized interface or output escaping (	AC-3, AC-6.
SI-11	Error Handling	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].	Organizations consider the structure and content of error messages. The extent to which systems	AU-2, AU-3, SC-31, SI-2, SI-15.
SI-12	Information Management and Retention	Manage and retain information within the system and information output from the system in acc	Information management and retention requirements cover the full life cycle of information, in so	AC-16, AU-5, AU-11, CA-2, CA-3, CA-5, CA-6, CA-7, CA-9, CM-5, CM-9, CP-2, IR-8, MP-2, MP-3, MP-4, MP-6, PL-2, PL-4, PM-4, PM-8, PM-9, PS-2, PS-6, PT-2, PT-3, RA-2, RA-3, SA-5, SA-8, SR-2.
SI-12(1)	Information Management and Retention | Limit Personally Identifiable Information Elements	Limit personally identifiable information being processed in the information life cycle to the follow	Limiting the use of personally identifiable information throughout the information life cycle when	PM-25.
SI-12(2)	Information Management and Retention | Minimize Personally Identifiable Information in Te	Use the following techniques to minimize the use of personally identifiable information for resear	Organizations can minimize the risk to an individual's privacy by employing techniques such as de-	PM-22, PM-25, SI-19.
SI-12(3)	Information Management and Retention | Information Disposal	Use the following techniques to dispose of, destroy, or erase information following the retention period: [Assignment: organization-defined techniques].	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.	None.
SI-13	Predictable Failure Prevention	a. Determine mean time to failure (MTTF) for the following system components in specific environments of operation: [Assignment: organization-defined system components]; and b. Provide substitute system components and a means to exchange active and standby components in accordance with the following criteria: [Assignment: organization-defined MTTF substitution criteria].	While MTTF is primarily a reliability issue, predictable failure prevention is intended to address po	CP-2, CP-10, CP-13, MA-2, MA-6, SA-8, SC-6.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
SI-13(1)	Predictable Failure Prevention | Transferring Component Responsibilities	Take system components out of service by transferring component responsibilities to substitute components no later than [Assignment: organization-defined fraction or percentage] of mean time to failure.	Transferring primary system component responsibilities to 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.	None.
SI-9	Information Input Restrictions	[Withdrawn: Incorporated into AC-2, AC-3, AC-5, and AC-6.]		
SI-13(3)	Predictable Failure Prevention | Manual Transfer Between Components	Manually initiate transfers between active and standby system components when the use of the active component reaches [Assignment: organization-defined percentage] of the mean time to failure.	For example, if the MTTF 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.	None.
SI-13(4)	Predictable Failure Prevention | Standby Component Installation and Notification	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]].	Automatic or manual transfer of components from standby to active mode can occur upon the detection of component failures.	None.
SI-13(5)	Predictable Failure Prevention | Failover Capability	Provide [Selection: real-time; near real-time] [Assignment: organization-defined failover capability	Failover refers to the automatic switchover to an alternate system upon the failure of the primary	CP-6, CP-7, CP-9.
SI-14	Non-persistence	Implement non-persistent [Assignment: organization-defined system components and services] th	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.	SC-30, SC-34, SI-21.
SI-14(1)	Non-persistence | Refresh from Trusted Sources	Obtain software and data employed during system component and service refreshes from the following trusted sources: [Assignment: organization-defined trusted sources].	Trusted sources include software and data from write-once, read-only media or from selected offline secure storage facilities.	None.
SI-14(2)	Non-persistence | Non-persistent Information	(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.	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.	None.
SI-14(3)	Non-persistence | Non-persistent Connectivity	Establish connections to the system on demand and terminate connections after [Selection: comp	Persistent connections to systems can provide advanced adversaries with paths to move laterally t	SC-10.
SI-15	Information Output Filtering	Validate information output from the following software programs and/or applications to ensure	Certain types of attacks, including SQL injections, produce output results that are unexpected or in	SI-3, SI-4, SI-11.
SI-16	Memory Protection	Implement the following controls to protect the system memory from unauthorized code executio	Some adversaries launch attacks with the intent of executing code in non-executable regions of m	AC-25, SC-3, SI-7.
SI-17	Fail-safe Procedures	Implement the indicated fail-safe procedures when the indicated failures occur: [Assignment: orga	Failure conditions include the loss of communications among critical system components or betwe	CP-12, CP-13, SC-24, SI-13.
SI-18	Personally Identifiable Information Quality Operations	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.	Personally identifiable information quality operations include the steps that organizations take to	PM-22, PM-24, PT-2, SI-4.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
SI-18(1)	Personally Identifiable Information Quality Operations | Automation Support	Correct or delete personally identifiable information that is inaccurate or outdated, incorrectly det	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.	PM-18, RA-8.
SI-18(2)	Personally Identifiable Information Quality Operations | Data Tags	Employ data tags to automate the correction or deletion of personally identifiable information acr	Data tagging personally identifiable information includes tags that note processing permissions, au	AC-3, AC-16, SC-16.
SI-18(3)	Personally Identifiable Information Quality Operations | Collection	Collect personally identifiable information directly from the individual.	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.	None.
SI-18(4)	Personally Identifiable Information Quality Operations | Individual Requests	Correct or delete personally identifiable information upon request by individuals or their designated representatives.	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.	None.
SI-18(5)	Personally Identifiable Information Quality Operations | Notice of Correction or Deletion	Notify [Assignment: organization-defined recipients of personally identifiable information] and individuals that the personally identifiable information has been corrected or deleted.	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.	None.
SI-19	De-identification	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.	De-identification is the general term for the process of removing the association between a set of	MP-6, PM-22, PM-23, PM-24, RA-2, SI-12.
SI-19(1)	De-identification | Collection	De-identify the dataset upon collection by not collecting personally identifiable information.	If a data source contains personally identifiable information but the information will not be used, the dataset can be de-identified 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.	None.
SI-19(2)	De-identification | Archiving	Prohibit archiving of personally identifiable information elements if those elements in a dataset will not be needed after the dataset is archived.	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.	None.
SI-19(3)	De-identification | Release	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.	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.	None.
SI-19(4)	De-identification | Removal, Masking, Encryption, Hashing, or Replacement of Direct Identifie	Remove, mask, encrypt, hash, or replace direct identifiers in a dataset.	There are many possible processes for removing direct identifiers from a dataset. Columns in a da	SC-12, SC-13.
SI-19(5)	De-identification | Statistical Disclosure Control	Manipulate numerical data, contingency tables, and statistical findings so that no individual or organization is identifiable in the results of the analysis.	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.	None.
SI-19(6)	De-identification | Differential Privacy	Prevent disclosure of personally identifiable information by adding non-deterministic noise to the	The mathematical definition for differential privacy holds that the result of a dataset analysis shou	SC-12, SC-13.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
SI-19(7)	De-identification | Validated Algorithms and Software	Perform de-identification using validated algorithms and software that is validated to implement the algorithms.	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.	None.
SI-19(8)	De-identification | Motivated Intruder	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.	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.	None.
SI-20	Tainting	Embed data or capabilities in the following systems or system components to determine if organiz	Many cyber-attacks target organizational information, or information that the organization holds	AU-13.
SI-21	Information Refresh	Refresh [Assignment: organization-defined information] at [Assignment: organization-defined fre	Retaining information for longer than it is needed makes it an increasingly valuable and enticing ta	SI-14.
SI-22	Information Diversity	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.	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.	None.
SI-23	Information Fragmentation	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].	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).	None.
SR-1	Policy and Procedures	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].	Supply chain risk management policy and procedures address the controls in the SR family as well	PM-9, PM-30, PS-8, SI-12.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
SR-2	Supply Chain Risk Management Plan	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.	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	CA-2, CP-4, IR-4, MA-2, MA-6, PE-16, PL-2, PM-9, PM-30, RA-3, RA-7, SA-8, SI-4.
SR-2(1)	Supply Chain Risk Management Plan | Establish SCRM Team	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].	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.	None.
SR-3	Supply Chain Controls and Processes	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]].	Supply chain elements include organizations, entities, or tools employed for the research and deve	CA-2, MA-2, MA-6, PE-3, PE-16, PL-8, PM-30, SA-2, SA-3, SA-4, SA-5, SA-8, SA-9, SA-10, SA-15, SC-7, SC-29, SC-30, SC-38, SI-7, SR-6, SR-9, SR-11.
SR-3(1)	Supply Chain Controls and Processes | Diverse Supply Base	Employ a diverse set of sources for the following system components and services: [Assignment: organization-defined system components and services].	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.	None.
SR-3(2)	Supply Chain Controls and Processes | Limitation of Harm	Employ the following controls to limit harm from potential adversaries identifying and targeting the organizational supply chain: [Assignment: organization-defined controls].	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.	None.

Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
SR-3(3)	Supply Chain Controls and Processes | Sub-tier Flow Down	Ensure that the controls included in the contracts of prime contractors are also included in the con	To manage supply chain risk effectively and holistically, it is important that organizations ensure th	SR-5, SR-8.
SR-4	Provenance	Document, monitor, and maintain valid provenance of the following systems, system components	Every system and system component has a point of origin and may be changed throughout its exis	CM-8, MA-2, MA-6, RA-9, SA-3, SA-8, SI-4.
SR-4(1)	Provenance | Identity	Establish and maintain unique identification of the following supply chain elements, processes, an	Knowing who and what is in the supply chains of organizations is critical to gaining visibility into su	IA-2, IA-8, PE-16.
SR-4(2)	Provenance | Track and Trace	Establish and maintain unique identification of the following systems and critical system compone	Tracking the unique identification of systems and system components during development and tra	IA-2, IA-8, PE-16, PL-2.
SR-4(3)	Provenance | Validate as Genuine and Not Altered	Employ the following controls to validate that the system or system component received is genuin	For many systems and system components, especially hardware, there are technical means to det	AT-3, SR-9, SR-10, SR-11.
SR-4(4)	Provenance | Supply Chain Integrity — Pedigree	Employ [Assignment: organization-defined controls] and conduct [Assignment: organization-defin	Authoritative information regarding the internal composition of system components and the prov	RA-3.
SR-5	Acquisition Strategies, Tools, and Methods	Employ the following acquisition strategies, contract tools, and procurement methods to protect a	The use of the acquisition process provides an important vehicle to protect the supply chain. Ther	AT-3, SA-2, SA-3, SA-4, SA-5, SA-8, SA-9, SA-10, SA-15, SR-6, SR-9, SR-10, SR-11.
SR-5(1)	Acquisition Strategies, Tools, and Methods | Adequate Supply	Employ the following controls to ensure an adequate supply of [Assignment: organization-defined	Adversaries can attempt to impede organizational operations by disrupting the supply of critical sy	RA-9.
SR-5(2)	Acquisition Strategies, Tools, and Methods | Assessments Prior to Selection, Acceptance, Mod	Assess the system, system component, or system service prior to selection, acceptance, modificati	Organizational personnel or independent, external entities conduct assessments of systems, comp	CA-8, RA-5, SA-11, SI-7.
SR-6	Supplier Assessments and Reviews	Assess and review the supply chain-related risks associated with suppliers or contractors and the s	An assessment and review of supplier risk includes security and supply chain risk management pro	SR-3, SR-5.
SR-6(1)	Supplier Assessments and Reviews | Testing and Analysis	Employ [Selection (one or more): organizational analysis; independent third-party analysis; organi	Relationships between entities and procedures within the supply chain, including development an	CA-8, SI-4.
SR-7	Supply Chain Operations Security	Employ the following Operations Security (OPSEC) controls to protect supply chain-related informa	Supply chain OPSEC expands the scope of OPSEC to include suppliers and potential suppliers. OPS	SC-38.
SR-8	Notification Agreements	Establish agreements and procedures with entities involved in the supply chain for the system, sys	The establishment of agreements and procedures facilitates communications among supply chain	IR-4, IR-6, IR-8.
SR-9	Tamper Resistance and Detection	Implement a tamper protection program for the system, system component, or system service.	Anti-tamper technologies, tools, and techniques provide a level of protection for systems, system	PE-3, PM-30, SA-15, SI-4, SI-7, SR-3, SR-4, SR-5, SR-10, SR-11.
SR-9(1)	Tamper Resistance and Detection | Multiple Stages of System Development Life Cycle	Employ anti-tamper technologies, tools, and techniques throughout the system development life c	The system development life cycle includes research and development, design, manufacturing, acq	SA-3.
SR-10	Inspection of Systems or Components	Inspect the following systems or system components [Selection (one or more): at random; at [Assi	The inspection of systems or systems components for tamper resistance and detection addresses	AT-3, PM-30, SI-4, SI-7, SR-3, SR-4, SR-5, SR-9, SR-11.
SR-11	Component Authenticity	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]].	Sources of counterfeit components include manufacturers, developers, vendors, and contractors.	PE-3, SA-4, SI-7, SR-9, SR-10.
SR-11(1)	Component Authenticity | Anti-counterfeit Training	Train [Assignment: organization-defined personnel or roles] to detect counterfeit system compon	None.	AT-3.
SR-11(2)	Component Authenticity | Configuration Control for Component Service and Repair	Maintain configuration control over the following system components awaiting service or repair a	None.	CM-3, MA-2, MA-4, SA-10.
SR-11(3)	Component Authenticity | Anti-counterfeit Scanning	Scan for counterfeit system components [Assignment: organization-defined frequency].	The type of component determines the type of scanning to be conducted (e.g., web application sc	RA-5.
SR-12	Component Disposal	Dispose of [Assignment: organization-defined data, documentation, tools, or system components]	Data, documentation, tools, or system components can be disposed of at any time during the syst	MP-6.