Markup Version of Special Publication 800-53 Revison 5, Initial Public Draft

This document reflects **significant changes to the controls, control enhancements, and supplemental guidance** between SP 800-53, Revision 4 and the Initial Public Draft of SP 800-53, Revision 5. The changes to the control baselines are reflected in a separate document.

The following changes are not tracked in this document:

- Formatting, structural, and editorial changes;
- Updates to related controls and references for each control;
- Removal of the "Priority Code" and "Baseline Allocation" for each control; and
- Addition of "Quick Links."

Note that many of the privacy controls are based on controls in the Privacy Appendix (Appendix J) of SP 800-53, Revision 4, but are dispayed as "new" in this document. For additional information and traceability of the privacy controls, please see Appendix F, Consolidated View of Privacy Controls.

ACCESS CONTROL

Quick link to Access Control summary table

AC-1 ACCESS CONTROL POLICY AND PROCEDURES

Control:

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

1. An 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. Reviews and updates the current:~~

b. Designate an [*Assignment: organization-defined senior management official*] to manage the access control policy and procedures;

c. Review and update the current access control:

1. Policy [*Assignment: organization-defined frequency*]; and

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

d. Ensure that the access control procedures implement the access control policy and controls; and

e. Develop, document, and implement remediation actions for violations of the access control policy.

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of ~~selected security~~ the controls and control enhancements in the AC

family. ~~Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance.~~ The risk management strategy is an important factor in establishing policy and procedures. Comprehensive policy and ~~guidance.~~procedures help provide security and privacy assurance. Security and privacy program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general security and privacy policy ~~for organizations or conversely,~~or can be represented by multiple policies reflecting the complex nature of ~~certain~~ organizations. The procedures can be established for security ~~program in general~~and privacy programs and for ~~particular information~~ systems, if needed. Procedures describe how policies or controls are implemented and can be directed at the personnel 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. It is important to recognize that restating controls does not constitute an organizational policy or procedure. ~~The organizational risk management strategy is a key factor in establishing policy and procedures.~~

Related Controls: IA-1, PM-9, PM-25, PS-8, SI-12.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-30, 800-39, 800-100; NIST Interagency Report 7874.

AC-2 ACCOUNT MANAGEMENT

Control:

a. ~~Identifies~~Define and ~~selects~~document the types of system accounts allowed for use within the system in support of organizational missions and business functions~~: [*Assignment: organization-defined information system account types*];~~;

b. Assign account managers for system accounts;

c. Establish conditions for group and role membership;

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

e. Require approvals by [*Assignment: organization-defined personnel or roles*] for requests to create system accounts;

f. Create, enable, modify, disable, and remove system accounts in accordance with [*Assignment: organization-defined policy, procedures, and conditions*];

g. Monitor the use of system accounts;

h. Notify account managers within [*Assignment: organization-defined time-period for each situation*]:

   1. When accounts are no longer required;

   2. When users are terminated or transferred; and

   3. When individual 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. Other attributes as required by the organization or associated missions and business functions;

j. Review accounts for compliance with account management requirements [*Assignment: organization-defined frequency*];

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

l. Align account management processes with personnel termination and transfer processes.

Supplemental Guidance: System account types include, for example, individual, shared, group, system, guest, anonymous, emergency, developer/manufacturer/vendor, temporary, and service. ~~Some of the account management requirements listed above can be implemented by organizational information systems.~~ The identification of authorized users of the system and the specification of access privileges reflects the requirements in other ~~security~~ controls in the security plan. Users requiring administrative privileges on system accounts receive additional scrutiny by appropriate organizational personnel responsible for approving such accounts and privileged access, including, for example, system owner, mission/business owner, or chief information security officer. Organizations may choose to define access privileges or other attributes by account, by type of account, or a combination of both. Other attributes required for authorizing access include, for example, restrictions on time-of-day, day-of-week, and point-of-origin. In defining other account attributes, organizations consider system-related requirements ~~(e.g., scheduled maintenance, system upgrades)~~ and mission/business requirements~~, (e.g., time zone differences, customer requirements, remote access to support travel requirements).~~ Failure to consider these factors could affect system availability.

Temporary and emergency accounts are intended for short-term use. Organizations establish temporary accounts as a part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation. Organizations establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes. Emergency and temporary accounts are not to be confused with infrequently used accounts including, for example, local logon accounts used for special tasks ~~defined by organizations~~ or when network resources are unavailable. Such accounts remain available and are not subject to automatic disabling or removal dates. Conditions for disabling or deactivating accounts include, for example, when shared/group, emergency, or temporary accounts are no longer required; or when individuals are transferred or terminated. Some types of system accounts may require specialized training.

Related Controls: AC-3, AC-5, AC-6, AC-17, AC-18, AC-20, AC-24, AU-9, CM-5, IA-2, IA-8, MA-3, MA-5, PE-2, PL-4, PS-2, PS-4, PS-5, PS-7, SC-7, SC-13, SC-37.

Control Enhancements:

(1) ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT MANAGEMENT

Employ automated mechanisms to support the management of system accounts.

Supplemental Guidance: The use of automated mechanisms can include, for example, using email or text messaging to automatically notify account managers when users are terminated or transferred; using the system to monitor account usage; and using telephonic notification to report atypical system account usage.

Related Controls: None.

(2) ACCOUNT MANAGEMENT | REMOVAL OF TEMPORARY AND EMERGENCY ACCOUNTS

Automatically [*Selection: remove; disable*] temporary and emergency accounts after [*Assignment: organization-defined time-period for each type of account*].

Supplemental Guidance: This control enhancement requires the removal or disabling of both temporary and emergency accounts automatically after a predefined time-period has elapsed, rather than at the convenience of the systems administrator. Automatic removal or disabling of accounts provides a more consistent implementation.

Related Controls: None.

(3) ACCOUNT MANAGEMENT | DISABLE ~~*INACTIVE*~~ ACCOUNTS

Automatically disable accounts ~~after~~when the accounts:

(a) Have expired;

(b) Are no longer associated to a user;

(c) Are in violation of organizational policy;

(d) Are no longer used by applications, services, or the system; and

~~(a)~~(e) Have been inactive for [*Assignment: organization-defined time period*].

Supplemental Guidance: None.

Related Controls: None.

(4) ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS

Automatically audit account creation, modification, enabling, disabling, and removal actions, and notify [*Assignment: organization-defined personnel or roles*].

Supplemental Guidance: None.

Related Controls: AU-2, AU-12.

(5) ACCOUNT MANAGEMENT | INACTIVITY LOGOUT

Require that users log out when [*Assignment: organization-defined time-period of expected inactivity or description of when to log out*].

Supplemental Guidance: This control enhancement is behavior/policy-based and requires users to take physical action to log out when they are expecting inactivity longer than the defined period.

Related Controls: AC-11.

(6) ACCOUNT MANAGEMENT | DYNAMIC PRIVILEGE MANAGEMENT

Implement the following dynamic privilege management capabilities: [*Assignment: organization-defined list of dynamic privilege management capabilities*].

Supplemental Guidance: In contrast to conventional access control approaches which employ static system accounts and predefined user privileges, dynamic access control approaches ~~(e.g., service-oriented architectures)~~ rely on run time access control decisions facilitated by dynamic privilege management such as attribute based access control (ABAC). While user identities remain relatively constant over time, user privileges typically change more frequently based on ongoing mission or business requirements and operational needs of organizations. Dynamic privilege management can include, for example, immediate revocation of privileges from users, as opposed to requiring that users terminate and restart their sessions to reflect any changes in privileges. Dynamic privilege management can also include those mechanisms that change user privileges based on dynamic rules as opposed to editing specific user profiles. Examples include automatic adjustments of user privileges if they are operating out of their normal work times, their job function or assignment changes, or if systems are under duress or in emergency ~~maintenance~~ situations. This control enhancement also includes the ~~ancillary~~ effects of privilege changes, for example, the changes to encryption keys used for communications~~. Dynamic privilege management can support requirements for information system resiliency~~.

Related Controls: AC-16.

(7) ACCOUNT MANAGEMENT | ROLE-BASED SCHEMES

(a) Establish and administer privileged user accounts in accordance with a role-based access scheme that organizes allowed system access and privileges into roles;

(b) Monitor privileged role assignments; and

(c) ~~Takes [*Assignment: organization-defined actions*]~~ Revoke access when privileged role assignments are no longer appropriate.

Supplemental Guidance: 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. These privileged roles include, for example, key management, account management, network and system administration, database administration, and web administration.

Related Controls: None.

(8) ACCOUNT MANAGEMENT | DYNAMIC ACCOUNT ~~*CREATION*~~MANAGEMENT

Create, activate, manage, and deactivate [*Assignment: organization-defined system accounts*] dynamically.

Supplemental Guidance: Approaches for dynamically creating, activating, managing, and deactivating system or service/application accounts ~~(e.g., as implemented within service-oriented architectures)~~ rely on ~~establishing~~ automatically provisioning the accounts ~~(identities)~~ at run time for entities that were previously unknown. Organizations plan for the dynamic creation, activation, management, and deactivation of these accounts by establishing trust relationships, business rules, and mechanisms with appropriate authorities to validate related authorizations and privileges.

Related Controls: AC-16.

(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*].

Supplemental Guidance: Before permitting the use of shared or group accounts, organizations consider the increased risk due to the lack of accountability with such accounts.

Related Controls: None.

(10) ACCOUNT MANAGEMENT | SHARED AND GROUP ACCOUNT CREDENTIAL ~~*TERMINATION*~~CHANGE

~~The information system terminates~~Change shared and group account credentials when members leave the group.

Supplemental Guidance: This control enhancement is intended to ensure that former group members do not retain access to the shared/group account.

Related Controls: None.

(11) ACCOUNT MANAGEMENT | USAGE CONDITIONS

Enforce [*Assignment: organization-defined circumstances and/or usage conditions*] for [*Assignment: organization-defined system accounts*].

Supplemental Guidance: This control enhancement helps to enforce the principle of least privilege, increase user accountability, and enable more effective account monitoring. Such monitoring includes, for example, alerts generated if the account is used outside of specified parameters. Organizations can describe the specific conditions or circumstances under which system accounts can be used, for example, by restricting usage to certain days of the week, time of day, or specific durations of time.

Related Controls: None.

(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*].

Supplemental Guidance: Atypical usage includes, for example, accessing systems at certain times of the day and from locations that are not consistent with the normal usage patterns of individuals working in organizations. Account monitoring may inadvertently create privacy risks. Data collected to identify atypical usage may reveal previously unknown information about the behavior of individuals. Organizations assess and document these risks in their privacy impact assessment and make determinations that are in alignment with their privacy program plan.

Related Controls: AU-6, AU-7, CA-7, IR-8, SI-4.

(13) ACCOUNT MANAGEMENT | DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS

Disable accounts of users posing a significant risk within [*Assignment: organization-defined time-period*] of discovery of the risk.

Supplemental Guidance: Users posing a significant risk to organizations include individuals for whom reliable evidence or intelligence indicates either the intention to use authorized access to systems to cause harm or through whom adversaries will cause harm. Such harm includes the potential adverse impacts to organizational operations and assets, individuals, other organizations, or the Nation. Close coordination and cooperation among authorizing officials,

system administrators, and human resource managers is essential for timely execution of this control enhancement.

Related Controls: AU-6, SI-4.

(14) ACCOUNT MANAGEMENT | PROHIBIT SPECIFIC ACCOUNT TYPES

Prohibit the creation and use of [*Selection (one or more): shared; guest; anonymous; temporary; emergency*] accounts for access to [*Assignment: organization-defined information types*].

Supplemental Guidance: NIST Special Publications 800-162, 800-178.

Related Controls: PS-4.

(15) ACCOUNT MANAGEMENT | ATTRIBUTE-BASED SCHEMES

(a) Establish and administer privileged user accounts in accordance with an attribute-based access scheme that specifies allowed system access and privileges based on attributes;

(b) Monitor privileged attribute-based assignments;

(c) Monitor changes to attributes; and

(d) Revoke access when privileged attribute-based assignments are no longer appropriate.

Supplemental Guidance: 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. These privileged roles include, for example, key management, account management, network and system administration, database administration, and web administration.

Related Controls: None.

References: NIST Special Publications 800-162, 800-178.

AC-3 ACCESS ENFORCEMENT

Control: Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

Supplemental Guidance: Access control policies ~~(e.g., identity-based policies, role-based policies, control matrices, cryptography)~~ control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (i.e., devices, files, records, domains) in organizational systems. In addition to enforcing authorized access at the system level and recognizing that systems can host many applications and services in support of organizational missions and business operations, access enforcement mechanisms can also be employed at the application and service level to provide increased information security.

Related Controls: 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, 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-25, PS-3, SC-2, SC-3, SC-4, SC-13, SC-28, SC-31, SC-34, SI-4.

Control Enhancements:

(1) ACCESS ENFORCEMENT | RESTRICTED ACCESS TO PRIVILEGED FUNCTIONS

[Withdrawn: Incorporated into AC-6].

(2) ACCESS ENFORCEMENT | DUAL AUTHORIZATION

Enforce dual authorization for [*Assignment: organization-defined privileged commands and/or other organization-defined actions*].

Supplemental Guidance: Dual authorization may also be known as two-person control. Dual authorization mechanisms require the approval of two authorized individuals to execute. Organizations do not require dual authorization mechanisms when immediate responses are necessary to ensure public and environmental safety.

Related Controls: CP-9, MP-6.

(3) ACCESS ENFORCEMENT | MANDATORY ACCESS CONTROL

Enforce [*Assignment: organization-defined mandatory access control policy*] over all subjects and objects where the policy:

(a) Is uniformly enforced across all subjects and objects within the boundary of the system;

(b) Specifies that a subject that has been granted access to information is constrained from doing any of the following;

(1) Passing the information to unauthorized subjects or objects;

(2) Granting its privileges to other subjects;

(3) Changing one or more security attributes on subjects, objects, the system, or system components;

(4) Choosing the security attributes and attribute values to be associated with newly created or modified objects; or

(5) Changing the rules governing access control; and

(c) Specifies that [*Assignment: organization-defined subjects*] may explicitly be granted [*Assignment: organization-defined privileges* ~~*(i.e., they are trusted subjects)*~~]] such that they are not limited by any of the above constraints.

Supplemental Guidance: Mandatory access control ~~as defined in this control enhancement is synonymous with~~is a type of nondiscretionary access control~~, and is not constrained only to certain historical uses (e.g., implementations using the Bell-LaPadula Model).~~. The above class of mandatory access control policies constrains what actions subjects can take with information obtained from data objects for which they have already been granted access. This prevents the subjects from passing the information to unauthorized subjects and objects. This class of mandatory access control policies also constrains what actions subjects can take with respect to the propagation of access control privileges; that is, a subject with a privilege cannot pass that privilege to other subjects. The policy is uniformly enforced over all subjects and objects to which the system has control. Otherwise, the access control policy can be circumvented. This enforcement ~~typically~~ is provided by an implementation that meets the reference monitor concept as described in AC-25. The policy is bounded by the system boundary (i.e., once the information is passed outside of the control of the system, additional means may be required to ensure that the constraints on the information remain in effect).

The trusted subjects described above are granted privileges consistent with the concept of least privilege (see AC-6). Trusted subjects are only given the minimum privileges relative to the above policy necessary for satisfying organizational mission/business needs. The control is most applicable when there is a policy mandate ~~(e.g., law, Executive Order, directive, or regulation)~~ that establishes a policy regarding access to ~~sensitive/~~controlled unclassified information or classified information and some users of the system are not authorized access to all such information resident in the system. This control can operate in conjunction with AC-3(4). A subject constrained in its operation by policies governed by this control is still able to operate under the less rigorous constraints of AC-3(4), but policies governed by this control take precedence over the less rigorous constraints of AC-3(4). For example, while a mandatory access control policy imposes a constraint preventing a subject from passing information to another subject operating at a different sensitivity label, AC-3(4) permits the subject to pass the information to any subject with the same sensitivity label as the subject.

Related Controls: SC-7.

(4) ACCESS ENFORCEMENT | DISCRETIONARY ACCESS CONTROL

Enforce [*Assignment: organization-defined discretionary access control policy*] over defined subjects and objects where the policy specifies that a subject that has been granted access to information can do one or more of the following:

(a) Pass the information to any other subjects or objects;

(b) Grant its privileges to other subjects;

(c) Change security attributes on subjects, objects, the system, or the system's components;

(d) Choose the security attributes to be associated with newly created or revised objects; or

(e) Change the rules governing access control.

Supplemental Guidance: When discretionary access control policies are implemented, subjects are not constrained regarding what actions they can take with information for which they have already been granted access. Thus, subjects that have been granted access to information are not prevented from passing (i.e., the subjects have the discretion to pass) the information to other subjects or objects. This control enhancement can operate in conjunction with AC-3(3). A subject that is constrained in its operation by policies governed by AC-3(3) is still able to

operate under the less rigorous constraints of this control enhancement. Therefore, while AC-3(3) imposes constraints preventing a subject from passing information to another subject operating at a different sensitivity level, AC-3(4) permits the subject to pass the information to any subject at the same sensitivity level. The policy is bounded by the system boundary. Once the information is passed outside of the control of the system, additional means may be required to help ensure that the constraints remain in effect. While the older, more traditional definitions of discretionary access control require identity-based access control, that limitation is not required for this use of discretionary access control.

Related Controls: None.

(5) ACCESS ENFORCEMENT | SECURITY-RELEVANT INFORMATION

Prevent access to [*Assignment: organization-defined security-relevant information*] except during secure, non-operable system states.

Supplemental Guidance: Security-relevant information is any information within systems that can potentially impact the operation of security functions or the provision of security services in a manner that could result in failure to enforce system security policies or maintain the isolation of code and data. Security-relevant information includes, for example, filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists. Secure, non-operable system states include the times in which systems are not performing mission/business-related processing, for example, the system is off-line for maintenance, troubleshooting, boot-up, or shut down.

Related Controls: CM-6, SC-39.

(6) ACCESS ENFORCEMENT | PROTECTION OF USER AND SYSTEM INFORMATION

[Withdrawn: Incorporated into MP-4 and SC-28].

(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*].

Supplemental Guidance: Role-based access control (RBAC) is an access control policy that restricts system access to authorized users. 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 the organizational 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 significant number of individuals for mid- to large-size organizations) but are instead acquired through role assignments. RBAC can be implemented either 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.

Related Controls: PE-2.

(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*].

Supplemental Guidance: Revocation of access rules may differ based on the types of access revoked. For example, if a subject (i.e., user or process) is removed from a group, access may not be revoked until the next time the object ~~(e.g., file)~~ is opened or the next time the subject attempts a new access to the object. Revocation based on changes to security labels may take effect immediately. Organizations ~~can~~ provide alternative approaches on how to make revocations immediate if systems cannot provide such capability and immediate revocation is necessary.

Related Controls: None.

(9) ACCESS ENFORCEMENT | CONTROLLED RELEASE

Release information outside of the established system boundary ~~unless~~only if:

(a) The receiving [*Assignment: organization-defined system or system component*] provides [*Assignment: organization-defined security safeguards*]; and

(b) [*Assignment: organization-defined security safeguards*] are used to validate the appropriateness of the information designated for release.

Supplemental Guidance: Systems can only protect organizational information within the confines of established system boundaries. Additional security ~~safeguards~~controls may be needed to ensure that such information is adequately protected once it is passed beyond the established system boundaries. ~~Examples of information leaving the system boundary include transmitting information to an external information system or printing the information on one of its printers.~~ In ~~cases~~situations where the system is unable to determine the adequacy of the protections provided by entities outside its boundary, as a mitigating control, organizations determine procedurally whether the external systems are providing adequate security. The means used to determine the adequacy of security provided by external systems include, for example, conducting inspections or periodic testing and assessments; 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 policy to protect the information.

This control enhancement requires systems to employ technical or procedural means to validate the information prior to releasing it to external systems. For example, if the system passes information to another system controlled by another organization, technical means are employed to validate that the security 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 appropriately authorized individuals gain access to the printer. This control enhancement is most applicable when there is some policy mandate that establishes policy regarding access to the information, and that policy applies beyond the realm of a particular system or organization.

Related Controls: SC-16.

(10) ACCESS ENFORCEMENT | AUDITED OVERRIDE OF ACCESS CONTROL MECHANISMS

Employ an audited override of automated access control mechanisms under [*Assignment: organization-defined conditions*] by [*Assignment: organization-defined roles*].

Supplemental Guidance: In certain situations, for example, where there is a threat to human life or an event that threatens the organization's ability carry out critical missions or business functions, an override capability for access control mechanisms may be needed. Such override conditions are defined by organizations and are used only in those limited circumstances.

Related Controls: AU-2, AU-6, AU-10, AU-12, AU-14.

(11) ACCESS ENFORCEMENT | RESTRICT ACCESS TO SPECIFIC INFORMATION

Restrict direct access to data repositories containing [*Assignment: organization-defined information types*].

Supplemental Guidance: This control enhancement is intended to provide flexibility regarding access control of specific pieces of information within a system. For example, role-based access could be employed to allow access to only a specific type of personally identifiable information within a database rather than allowing access to the database in its entirety.

Related Controls: None.

(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*]; and

(b) Provide an enforcement mechanism to prevent other-than-asserted access.

Supplemental Guidance: This control enhancement is intended to address applications that need to access existing system applications and functions including, for example, user contacts; global positioning system; camera; keyboard; microphone; network; or phones or other files.

Related Controls: CM-7.

(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*].

Supplemental Guidance: Attribute-based access control (ABAC) is an access control policy that restricts system access to authorized users based on their organizational attributes, such as job function; environmental attributes, such as time of day; and resource attributes, such as the classification of a document. Organizations can create specific rules based on attributes and the authorizations (i.e., privileges) to perform needed operations on the systems associated with the organization-defined attributes and rules. When users are assigned to attributes defined in ABAC policies or rules, they can be provisioned to a system with appropriate privileges or dynamically granted access to a protected resource upon access. ABAC can be implemented either as a mandatory or discretionary form of access control. For organizations implementing ABAC with mandatory access controls, the requirements in AC-3(3) define the scope of the subjects and objects covered by the policy.

Related Controls: PE-2.

References: NIST Special Publications 800-57-1, 800-57-2, 800-57-3, 800-162; NIST Interagency Report 7874.

AC-4 INFORMATION FLOW ENFORCEMENT

Control: Enforce approved authorizations for controlling the flow of information within the system and between interconnected systems based on [*Assignment: organization-defined information flow control policies*].

Supplemental Guidance: Information flow control regulates where information ~~is allowed to~~can travel within a system and between systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. Flow control restrictions include, for example, keeping export-controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization, restricting web requests to the Internet that are not from the internal web proxy server, and limiting information transfers between organizations based on data structures and content. Transferring information between systems ~~representing~~in different security domains with different security policies introduces risk that such transfers violate one or more domain security policies. In such situations, information owners or stewards provide guidance at designated policy enforcement points between interconnected systems. Organizations consider mandating specific architectural solutions when required to enforce specific security policies. Enforcement includes, for example, prohibiting information transfers between interconnected systems (i.e., allowing access only); employing hardware mechanisms to enforce one-way information flows; and implementing trustworthy regrading mechanisms to reassign security attributes and security labels.

Organizations commonly employ information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations ~~(e.g., networks, individuals, and devices)~~ within systems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Enforcement occurs, for example, in boundary protection devices ~~(e.g., gateways, routers, guards, encrypted tunnels, firewalls)~~ that employ rule sets or establish configuration settings that restrict system services, provide a packet-filtering capability based on header information, or message-filtering capability based on message content ~~(e.g., implementing key word searches or using document characteristics).~~ Organizations also consider the trustworthiness of filtering/inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement. Control enhancements 3 through 22 primarily address cross-domain solution needs which focus on more advanced filtering techniques, in-depth analysis, and stronger flow enforcement mechanisms implemented in cross-domain products, for example, high-assurance guards. Such capabilities are generally not available in commercial off-the-shelf information technology products.

Related Controls: AC-3, AC-6, AC-16, AC-17, AC-19, AC-21, AU-10, CA-9, CM-7, PM-25, SC-4, SC-7, SC-16, SC-31.

Control Enhancements:

(1) INFORMATION FLOW ENFORCEMENT | OBJECT SECURITY ATTRIBUTES

Use [*Assignment: organization-defined security 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.

Supplemental Guidance: Information flow enforcement mechanisms compare security attributes associated with information (data content and data structure) and source/destination objects, and respond appropriately ~~(e.g., block, quarantine, alert administrator)~~ when the 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*. Security attributes can also include, for example, source and destination addresses employed in traffic filter firewalls. Flow enforcement using explicit security attributes can be used, for example, to control the release of certain types of information.

Related Controls: None.

(2) INFORMATION FLOW ENFORCEMENT | PROCESSING DOMAINS

Use protected processing domains to enforce [*Assignment: organization-defined information flow control policies*] as a basis for flow control decisions.

Supplemental Guidance: Within systems, protected processing domains are processing spaces that have controlled interactions with other processing spaces, enabling control of information flows between these spaces and to/from data/information objects. A protected processing domain can be provided, for example, by implementing domain and type enforcement. In domain and type enforcement, system processes are assigned to domains; information is identified by types; and information flows are controlled based on allowed information accesses (determined by domain and type), allowed signaling among domains, and allowed process transitions to other domains.

Related Controls: SC-39.

(3) INFORMATION FLOW ENFORCEMENT | DYNAMIC INFORMATION FLOW CONTROL

Enforce dynamic information flow control based on [*Assignment: organization-defined policies*].

Supplemental Guidance: Organizational policies regarding dynamic information flow control include, for example, allowing or disallowing information flows based on changing conditions or mission/operational considerations. Changing conditions include, for example, changes in organizational risk tolerance due to changes in the immediacy of mission/business needs, changes in the threat environment, and detection of potentially harmful or adverse events.

Related Controls: SI-4.

(4) INFORMATION FLOW ENFORCEMENT ~~| *CONTENT CHECK*~~ | FLOW CONTROL OF ENCRYPTED INFORMATION

Prevent encrypted information from bypassing ~~content checking~~[*Assignment: organization-defined flow control mechanisms*] by [*Selection (one or more): decrypting the information; blocking the flow of the encrypted information; terminating communications sessions attempting to pass encrypted information; [Assignment: organization-defined procedure or method*]].

Supplemental Guidance: Content checking, security policy filters, and data type identifiers are examples of flow control mechanisms.

Related Controls: SI-4.

(5) INFORMATION FLOW ENFORCEMENT | EMBEDDED DATA TYPES

Enforce [*Assignment: organization-defined limitations*] on embedding data types within other data types.

Supplemental Guidance: Embedding data types within other data types may result in reduced flow control effectiveness. Data type embedding includes, for example, inserting executable files as objects within word processing files, inserting references or descriptive information

into a media file, and 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.

Related Controls: None.

(6) INFORMATION FLOW ENFORCEMENT | METADATA

Enforce information flow control based on [*Assignment: organization-defined metadata*].

Supplemental Guidance: Metadata is information used to describe the characteristics of data. Metadata can include structural metadata describing data structures ~~(e.g., data format, syntax, and semantics)~~ or descriptive metadata describing data contents ~~(e.g., age, location, telephone number).~~ Enforcing allowed information flows based on metadata enables simpler and more effective flow control. Organizations consider the trustworthiness of metadata regarding data accuracy (i.e., knowledge that the metadata values are correct with respect to the data), data integrity (i.e., protecting against unauthorized changes to metadata tags), and the binding of metadata to the data payload (i.e., ensuring sufficiently strong binding techniques with appropriate levels of assurance).

Related Controls: AC-16, SI-7.

(7) INFORMATION FLOW ENFORCEMENT | ONE-WAY FLOW MECHANISMS

Enforce [*Assignment: organization-defined one-way information flows*] using hardware mechanisms.

Supplemental Guidance: None.

Related Controls: None.

(8) INFORMATION FLOW ENFORCEMENT | SECURITY POLICY FILTERS

Enforce information flow control using [*Assignment: organization-defined security policy filters*] as a basis for flow control decisions for [*Assignment: organization-defined information flows*].

Supplemental Guidance: Organization-defined security policy filters can address data structures and content. For example, security policy filters for data structures can check for maximum file lengths, maximum field sizes, and data/file types (for structured and unstructured data). Security policy filters for data content can check for specific words ~~(e.g., dirty/clean word filters),~~ enumerated values or data value ranges, and hidden content. Structured data permits the interpretation of data content by applications. Unstructured data ~~typically~~ refers to digital information without a ~~particular~~ data structure or with a data structure that does not facilitate the development of rule sets to address the ~~particular~~ sensitivity of the information conveyed by the data or the ~~associated~~ 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 ~~(e.g., commercial off-the-shelf word processing documents, spreadsheets, or emails).~~ Organizations can implement more than one security policy filter to meet information flow control objectives ~~(e.g., employing clean word lists in conjunction with dirty word lists may help to reduce false positives).~~

Related Controls: None.

(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*].

Supplemental Guidance: Organizations define security 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 policy filtering. Human reviews may also be employed as deemed necessary by organizations.

Related Controls: None.

(10) INFORMATION FLOW ENFORCEMENT | ENABLE AND DISABLE SECURITY POLICY FILTERS

Provide the capability for privileged administrators to enable and disable [*Assignment: organization-defined security policy filters*] under the following conditions: [*Assignment: organization-defined conditions*].

Supplemental Guidance: For example, as allowed by the system authorization, administrators can enable security policy filters to accommodate approved data types.

Related Controls: None.

(11) INFORMATION FLOW ENFORCEMENT | CONFIGURATION OF SECURITY POLICY FILTERS

Provide the capability for privileged administrators to configure [*Assignment: organization-defined security policy filters*] to support different security policies.

Supplemental Guidance: For example, to reflect changes in security policies, administrators can change the list of "dirty words" that security policy mechanisms check in accordance with the definitions provided by organizations.

Related Controls: None.

(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.

Supplemental Guidance: Data type identifiers include, for example, filenames, file types, file signatures/tokens, and multiple internal file signatures/tokens. Systems may allow transfer of data only if compliant with data type format specifications.

Related Controls: None.

(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.

Supplemental Guidance: 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. Parsing transfer files facilitates policy decisions on source, destination, certificates, classification, attachments, and other security-related component differentiators.

Related Controls: None.

(14) INFORMATION FLOW ENFORCEMENT | SECURITY POLICY FILTER CONSTRAINTS

When transferring information between different security domains, implement [*Assignment: organization-defined security policy filters*] requiring fully enumerated formats that restrict data structure and content.

Supplemental Guidance: Data structure and content restrictions reduce the range of potential malicious or unsanctioned content in cross-domain transactions. Security policy filters that restrict data structures include, for example, restricting file sizes and field lengths. Data content policy filters include, for example, encoding formats for character sets ~~(e.g., Universal Character Set Transformation Formats, American Standard Code for Information Interchange)~~; restricting character data fields to only contain alpha-numeric characters; prohibiting special characters; and validating schema structures.

Related Controls: None.

(15) INFORMATION FLOW ENFORCEMENT | DETECTION OF UNSANCTIONED INFORMATION

When transferring information between different security domains, examine the information for the presence of [*Assignment: organized-defined unsanctioned information*] and prohibit the transfer of such information in accordance with the [*Assignment: organization-defined security policy*].

Supplemental Guidance: Detection of unsanctioned information includes, for example, checking all information to be transferred for malicious code and dirty words.

Related Controls: SI-3.

(16) INFORMATION FLOW ENFORCEMENT | INFORMATION TRANSFERS ON INTERCONNECTED SYSTEMS

[Withdrawn: Incorporated into AC-4].

(17) INFORMATION FLOW ENFORCEMENT | DOMAIN AUTHENTICATION

Uniquely identify and authenticate source and destination points by [*Selection (one or more): organization, system, application, service, individual*] for information transfer.

Supplemental Guidance: Attribution is a critical component of a security concept of operations. The ability to identify source and destination points for information flowing in systems, allows the forensic reconstruction of events when required, and encourages policy compliance by attributing policy violations to specific organizations/individuals. Successful domain authentication requires that system labels distinguish among systems, organizations, and individuals involved in preparing, sending, receiving, or disseminating information.

Related Controls: IA-2, IA-3, IA-9.

(18) INFORMATION FLOW ENFORCEMENT | SECURITY ATTRIBUTE BINDING

~~**The information system binds security attributes to information using [*Assignment: organization-defined binding techniques*] to facilitate information flow policy enforcement.**~~

Supplemental Guidance: ~~Binding techniques implemented by information systems affect the strength of security attribute binding to information.~~[Withdrawn: Incorporated into AC-16].

~~**(19)** Binding strength and the assurance associated with binding techniques play an important part in the trust organizations have in the information flow enforcement process. The binding techniques affect the number and degree of additional reviews required by organizations.~~ ~~Related controls: AC-16, SC-16.~~

~~**(20)**~~**(19)** INFORMATION FLOW ENFORCEMENT | VALIDATION OF METADATA

When transferring information between different security domains, apply the same security policy filtering to metadata as it applies to data payloads.

Supplemental Guidance: This control enhancement requires the validation of metadata and the data to which the metadata applies. 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, considering metadata and the data to which the metadata applies as part of the payload. All information (including metadata and the data to which the metadata applies) is subject to filtering and inspection.

Related Controls: None.

~~**(21)**~~**(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.

Supplemental Guidance: Organizations define approved solutions and configurations in cross-domain policies and guidance in accordance with the types of information flows across classification boundaries. The Unified Cross Domain Management Office provides a baseline listing of approved cross-domain solutions.

Related Controls: None.

~~**(22)**~~**(21)** INFORMATION FLOW ENFORCEMENT | PHYSICAL AND LOGICAL SEPARATION OF INFORMATION FLOWS

Separate information flows logically or physically using [*Assignment: organization-defined mechanisms and/or techniques*] to accomplish [*Assignment: organization-defined required separations by types of information*].

Supplemental Guidance: Enforcing the separation of information flows by type can enhance protection by ensuring that information is not commingled while in transit and by enabling flow control by transmission paths perhaps not otherwise achievable. Types of separable information include, for example, inbound and outbound communications traffic, service requests and responses, and information of differing security categories.

Related Controls: SC-32.

~~**(23)**~~**(22)** INFORMATION FLOW ENFORCEMENT | ACCESS ONLY

Provide access from a single device to computing platforms, applications, or data residing on multiple different security domains, while preventing any information flow between the different security domains.

Supplemental Guidance: The system, for example, provides a desktop for users to access each connected security domain without providing any mechanisms to allow transfer of information between the different security domains.

Related Controls: None.

References: NIST Special Publications 800-162, 800-178.

AC-5 SEPARATION OF DUTIES

Control:

a. Separate [*Assignment: organization-defined duties of individuals*];

b. Document separation of duties of individuals; and

c. Define system access authorizations to support separation of duties.

Supplemental Guidance: Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example, dividing mission functions and system support functions among different individuals and/or roles; conducting system support functions with different individuals ~~(e.g., system management, programming, configuration management, quality assurance;~~ and ~~testing, and network security);~~ ensuring security personnel administering access control functions do not also administer audit functions. Because separation of duty violations can span systems and application domains, organizations consider the entirety of organizational systems and system components when developing policy on separation of duties.

Related Controls: AC-2, AC-3, AC-6, AU-9, CM-5, CM-11, CP-9, IA-2, IA-5, MA-3, MA-5, PS-2, SA-17.

Control Enhancements: None.

References: None.

AC-6 LEAST PRIVILEGE

Control: Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

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

Related Controls: AC-2, AC-3, AC-5, AC-16, CM-5, CM-11, PL-2, PM-12, SA-15, SA-17, SC-38.

Control Enhancements:

(1) LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS

Explicitly authorize access to [*Assignment: organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information*].

Supplemental Guidance: Security functions include, for example, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and ~~setting~~establishing intrusion detection parameters. Security-relevant information includes, for example, filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists. Explicitly authorized personnel include, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users.

Related Controls: AC-17, AC-18, AC-19, AU-9, PE-2.

(2) LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS

Require that users of system accounts, or roles, with access to [*Assignment: organization-defined security functions or security-relevant information*], use non-privileged accounts or roles, when accessing nonsecurity functions.

Supplemental Guidance: This control enhancement limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations implement access control policies such as role-based access control and where a change of role provides the same degree of assurance in the change of access authorizations for both the user and all processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account.

Related Controls: AC-17, AC-18, AC-19, PL-4.

(3) LEAST PRIVILEGE | NETWORK ACCESS TO PRIVILEGED COMMANDS

Authorize network access to [*Assignment: organization-defined privileged commands*] only for [*Assignment: organization-defined compelling operational needs*] and document the rationale for such access in the security plan for the system.

Supplemental Guidance: Network access is any access across a network connection in lieu of local access (i.e., user being physically present at the device).

Related Controls: AC-17, AC-18, AC-19.

(4) LEAST PRIVILEGE | SEPARATE PROCESSING DOMAINS

Provide separate processing domains to enable finer-grained allocation of user privileges.

Supplemental Guidance: Providing separate processing domains for finer-grained allocation of user privileges includes, for example, using virtualization techniques to allow additional user privileges within a virtual machine while restricting privileges to other virtual machines or to the underlying actual machine; employing hardware/software domain separation mechanisms; and implementing separate physical domains.

Related Controls: AC-4, SC-2, SC-3, SC-30, SC-32, SC-39.

(5) LEAST PRIVILEGE | PRIVILEGED ACCOUNTS

Restrict privileged accounts on the system to [*Assignment: organization-defined personnel or roles*].

Supplemental Guidance: Privileged accounts, including super user accounts, are typically described as system administrator for various types of commercial off-the-shelf operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from having access to privileged information/functions. Organizations may differentiate in the application of this control enhancement between allowed privileges for local accounts and for domain accounts provided they retain the ability to control system configurations for key security parameters and as otherwise necessary to sufficiently mitigate risk.

Related Controls: IA-2, MA-3, MA-4.

(6) LEAST PRIVILEGE | PRIVILEGED ACCESS BY NON-ORGANIZATIONAL USERS

Prohibit privileged access to the system by non-organizational users.

Supplemental Guidance: None.

Related Controls: AC-18, AC-19, IA-2, IA-8.

(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.

Supplemental Guidance: The need for certain assigned user privileges may change over time reflecting changes in organizational missions and business functions, environments of operation, technologies, or threat. Periodic review of assigned user privileges is necessary to determine if the rationale for assigning such privileges remains valid. If the need cannot be revalidated, organizations take appropriate corrective actions.

Related Controls: CA-7.

(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*].

Supplemental Guidance: In certain situations, software applications/programs need to execute with elevated privileges to perform required functions. However, if the privileges required for execution are at a higher level than the privileges assigned to organizational users invoking such applications/programs, those users are indirectly provided with greater privileges than assigned by organizations.

Related Controls: None.

(9) LEAST PRIVILEGE | AUDITING USE OF PRIVILEGED FUNCTIONS

Audit the execution of privileged functions.

Supplemental Guidance: Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Auditing the use of privileged functions is one way to detect such misuse, and in doing so, help mitigate the risk from insider threats and the advanced persistent threat.

Related Controls: AU-2, AU-12.

(10) LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS

Prevent non-privileged users from executing privileged functions.

Supplemental Guidance: Privileged functions include, for example, disabling, circumventing, or altering implemented security or privacy controls, establishing system accounts, performing system integrity checks, or administering cryptographic key management activities. Non-privileged users are individuals that do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users.

Related Controls: None.

References: None.

AC-7 UNSUCCESSFUL LOGON ATTEMPTS

Control:

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/node for an* [*Assignment: organization-defined time-period*]; *lock the account/node until released by an administrator; delay next logon prompt per* [*Assignment: organization-defined delay algorithm*]; take [*Assignment: organization-defined action*]] when the maximum number of unsuccessful attempts is exceeded.

Supplemental Guidance: This control applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by systems are usually temporary and automatically release after a predetermined time established by organizations. If a delay algorithm is selected, organizations may employ different algorithms for different components of the system based on the capabilities of those components. Responses to unsuccessful logon attempts may be implemented at both the operating system and the application levels.

Related Controls: AC-2, AC-9, AU-2, AU-6, IA-5.

Control Enhancements:

(1) UNSUCCESSFUL LOGON ATTEMPTS | AUTOMATIC ACCOUNT LOCK

[Withdrawn: Incorporated into AC-7].

(2) UNSUCCESSFUL LOGON ATTEMPTS | PURGE OR WIPE MOBILE DEVICE

Purge or wipe information from [*Assignment: organization-defined mobile devices*] based on [*Assignment: organization-defined purging or wiping requirements and techniques*] after [*Assignment: organization-defined number*] consecutive, unsuccessful device logon attempts.

Supplemental Guidance: This control enhancement applies only to mobile devices for which a logon occurs ~~(e.g., personal digital assistants, smart phones, tablets).~~ The logon is to the mobile device, not to any one account on the device. Successful logons to ~~any~~ accounts on mobile devices reset the unsuccessful logon count to zero. ~~Organizations define information to be purged/wiped carefully in order to avoid over purging/wiping which may result in devices becoming unusable.~~ Purging or wiping may be unnecessary if the information on the device is protected with sufficiently strong encryption mechanisms.

Related Controls: AC-19, MP-5, MP-6.

(3) UNSUCCESSFUL LOGON ATTEMPTS | BIOMETRIC ATTEMPT LIMITING

Limit the number of unsuccessful biometric logon attempts to [*Assignment: organization-defined number*].

Supplemental Guidance: Biometrics are probabilistic in nature. The ability to successfully authenticate can be impacted by many factors, including matching performance and presentation attack detection mechanisms. Organizations select the appropriate number of attempts and fall back mechanisms for users based on these, and other organizationally defined factors.

Related Controls: IA-3.

(4) UNSUCCESSFUL LOGON ATTEMPTS | USE OF ALTERNATE FACTOR

Allow the use of one or more additional authentication factors after the number of organization-defined consecutive invalid logon attempts have been exceeded.

Supplemental Guidance: This control enhancement supports the objective of availability and allows a user that has inadvertently been locked out to use additional authentication factors to bypass the lockout.

Related Controls: IA-3.

References: NIST Special Publications 800-63, 800-124.

AC-8 SYSTEM USE NOTIFICATION

Control:

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, policies, regulations, 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.

Supplemental Guidance: System use notifications can be implemented using messages or warning banners displayed before individuals log in to systems. System use notifications are used only for

access via logon interfaces with human users. Such notifications are not required when human interfaces do not exist. Based on an assessment of risk, organizations consider whether or not a secondary system use notification is needed to access applications or other system resources after the initial network logon. Organizations consider system use notification messages or banners displayed in multiple languages based on ~~specific~~ organizational needs and the demographics of ~~information~~ system users. Organizations also consult with the Office of the General Counsel for legal review and approval of warning banner content.

Related Controls: AC-14, PL-4, SI-4.

Control Enhancements: None.

References: None.

AC-9 PREVIOUS LOGON (ACCESS) NOTIFICATION

Control: Notify the user, upon successful logon (access) to the system, of the date and time of the last logon (access).

Supplemental Guidance: This control is applicable to logons to systems via human user interfaces and logons to systems that occur in other types of architectures ~~(e.g., service-oriented architectures).~~ .

Related Controls: AC-7, PL-4.

Control Enhancements:

(1) PREVIOUS LOGON NOTIFICATION | UNSUCCESSFUL LOGONS

Notify the user, upon successful logon/access, of the number of unsuccessful logon/access attempts since the last successful logon/access.

Supplemental Guidance: None.

Related Controls: None.

(2) PREVIOUS LOGON NOTIFICATION | SUCCESSFUL AND UNSUCCESSFUL LOGONS

Notify the user, upon successful logon/access, of the number of [*Selection: successful logons/accesses; unsuccessful logon/access attempts; both*] during [*Assignment: organization-defined time-period*].

Supplemental Guidance: None.

Related Controls: None.

(3) PREVIOUS LOGON NOTIFICATION | NOTIFICATION OF ACCOUNT CHANGES

Notify the user, upon successful logon/access, of changes to [*Assignment: organization-defined security-related characteristics/parameters of the user's account*] during [*Assignment: organization-defined time-period*].

Supplemental Guidance: None.

Related Controls: None.

(4) PREVIOUS LOGON NOTIFICATION | ADDITIONAL LOGON INFORMATION

Notify the user, upon successful logon/access, of the following additional information: [*Assignment: organization-defined information to be included in addition to the date and time of the last logon/access*].

Supplemental Guidance: This control enhancement permits organizations to specify additional information to be provided to users upon logon including, for example, the location of last logon. User location is defined as that information which can be determined by systems, for example, Internet Protocol (IP) addresses from which network logons occurred, notifications of local logons, or device identifiers.

Related Controls: None.

References: None.

AC-10 CONCURRENT SESSION CONTROL

Control: Limit the number of concurrent sessions for each [*Assignment: organization-defined account and/or account type*] to [*Assignment: organization-defined number*].

Supplemental Guidance: Organizations may define the maximum number of concurrent sessions for system accounts globally, by account type ~~(e.g., privileged user, non-privileged user, domain, specific application),~~ by account, or a combination thereof. For example, organizations may limit the number of concurrent sessions for system administrators or other individuals working in particularly sensitive domains or mission-critical applications. This control addresses concurrent sessions for system accounts and does not address concurrent sessions by single users via multiple system accounts.

Related Controls: SC-23.

Control Enhancements: None.

References: None.

AC-11 ~~SESSION~~DEVICE LOCK

Control:

a. Prevent further access to the system by initiating a device lock after [*Assignment: organization-defined time-period*] of inactivity or upon receiving a request from a user; and

b. Retain the ~~session~~device lock until the user reestablishes access using established identification and authentication procedures.

Supplemental Guidance: ~~Session~~Device locks are temporary actions taken to prevent logical access to organizational systems when users stop work and move away from the immediate vicinity of those systems but do not want to log out because of the temporary nature of their absences. ~~Session~~Device locks are implemented where session activities can be determined. This is typically at the operating system level, but can also be at the application level. ~~Session~~Device locks are not an acceptable substitute for logging out of systems, for example, if organizations require users to log out at the end of workdays.

Related Controls: AC-2, AC-7, IA-11.

Control Enhancements:

(1) ~~*SESSION*~~DEVICE LOCK | PATTERN-HIDING DISPLAYS

Conceal, via the ~~session~~device lock, information previously visible on the display with a publicly viewable image.

Supplemental Guidance: ~~Publicly viewable images~~The pattern-hiding display can include static or dynamic images, for example, patterns used with screen savers, photographic images, solid colors, clock, battery life indicator, or a blank screen, with the ~~additional~~ caveat that ~~none of the images convey sensitive~~controlled unclassified information is not displayed.

Related Controls: None.

(2) DEVICE LOCK | REQUIRE USER-INITIATED LOCK

Require the user to initiate a device lock before leaving the system unattended.

Supplemental Guidance: This control enhancement is behavior/policy-based and as such, requires users to take physical action to initiate the device lock.

Related Controls: PL-4.

References: None.

AC-12 SESSION TERMINATION

Control: Automatically terminate a user session after [*Assignment: organization-defined conditions or trigger events requiring session disconnect*].

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

Related Controls: MA-4, SC-10, SC-23.

Control Enhancements:

(1) SESSION TERMINATION | USER-INITIATED LOGOUTS ~~/ *MESSAGE DISPLAYS*~~

Provide a logout capability for user-initiated communications sessions whenever authentication is used to gain access to [*Assignment: organization-defined information resources*].

~~**(1) Displays an explicit logout message to users indicating the reliable termination of authenticated communications sessions.**~~

Supplemental Guidance: Information resources to which users gain access via authentication include, for example, local workstations, databases, and password-protected websites/web-based services.

Related Controls: None.

(2) SESSION TERMINATION | TERMINATION MESSAGE

Display an explicit logout message to users indicating the reliable termination of authenticated communications sessions.

Supplemental Guidance: Logout messages for web page access, for example, can be displayed after authenticated sessions have been terminated. However, for some types of interactive sessions including, for example, file transfer protocol (FTP) sessions, systems typically send logout messages as final messages prior to terminating sessions.

Related Controls: None.

(3) SESSION TERMINATION | TIMEOUT WARNING MESSAGE

Display an explicit message to users indicating that the session is about to end.

Supplemental Guidance: To increase usability, notify users of pending session termination and prompt for activity if users desire to continue the session.

Related Controls: None.

References: None.

AC-13 SUPERVISION AND REVIEW — ACCESS CONTROL

[Withdrawn: Incorporated into AC-2 and AU-6].

AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

Control:

a. Identify [*Assignment: organization-defined user actions*] that can be performed on the system without identification or authentication consistent with organizational missions and business functions; and

b. Document and provide supporting rationale in the security plan for the system, user actions not requiring identification or authentication.

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

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

Related Controls: AC-8, IA-2, PL-2.

Control Enhancements: None.

(1) PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION | NECESSARY USES
[Withdrawn: Incorporated into AC-14].

References: None.

AC-15 AUTOMATED MARKING

[Withdrawn: Incorporated into MP-3].

AC-16 SECURITY AND PRIVACY ATTRIBUTES

Control:

a. Provide the means to associate [*Assignment: organization-defined types of security and privacy attributes*] having [*Assignment: organization-defined security and privacy attribute values*] with information in storage, in process, and/or in transmission;

b. Ensure that the security and privacy attribute associations are made and retained with the information;

c. Establish the permitted [*Assignment: organization-defined security attributes*] for [*Assignment: organization-defined systems*]; and

d. Determine the permitted [*Assignment: organization-defined values or ranges*] for each of the established security and privacy attributes.

Supplemental Guidance: 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 representing 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 an entity with respect to the management of personally identifiable information. Such attributes are used to enable the implementation of the need for the record in the performance of duties, the identification of personal information within data objects, and the identification of permitted uses of personal information. Attributes can be explicitly or implicitly associated with the information contained in organizational systems or system components.

Security and privacy attributes may be associated with active entities (i.e., subjects) that have the potential to send or receive information, to cause information to flow among objects, or to change the system state. These attributes may also be associated with passive entities (i.e., objects) that contain or receive information. The association of security and privacy attributes to subjects and objects is referred to as binding and is inclusive of setting the attribute value and the attribute type. Security and privacy attributes when bound to data or information, enable the enforcement of

security policies for access control and information flow control and privacy policies including, for example, for data retention limits and permitted uses of personally identifiable information. Such enforcement occurs through organizational processes or system functions or mechanisms. Binding techniques implemented by systems affect the strength of attribute binding to information. Binding strength and the assurance associated with binding techniques play an important part in the trust 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 the security and privacy attributes can directly affect the ability of individuals to access organizational information.

Organizations can define the types of attributes needed for selected systems to support missions or business functions. There is potentially a wide range of values that can be assigned to any given security attribute. Release markings can include, for example, US only, NATO, or NOFORN (not releasable to foreign nationals). By specifying permitted attribute ranges and values, organizations ensure that the security and privacy attribute values are meaningful and relevant. ~~The term *security* Labeling~~ refers to the association of security and privacy attributes with subjects and objects represented by the internal data structures within organizational systems. This facilitates system-based enforcement of information security and privacy policies. ~~Security~~ Labels include, for example, access authorizations, nationality, data life cycle protection (i.e., encryption and data expiration), data subject consents, permissible data uses, affiliation as contractor, and classification of information in accordance with legal and compliance requirements. Conversely, marking refers to the association of security and privacy attributes with objects in a human-readable form. This enables manual, procedural, or process-based enforcement of information security and privacy policies. ~~The AC-16 base control represents the requirement for user-based attribute association (marking). The enhancements to AC-16 represent additional requirements including information system-based attribute association (labeling~~Examples of attribute types include classification level for objects and clearance (access authorization) level for subjects. An ~~example of a~~attribute value for both attribute types is *Top Secret*.

Related Controls: AC-3, AC-4, AC-6, AC-21, AC-25, AU-2, AU-10, IP-2, MP-3, PE-22, SC-11, SC-16, SI-12.

Control Enhancements:

(1) SECURITY AND PRIVACY ATTRIBUTES | DYNAMIC ATTRIBUTE ASSOCIATION

Dynamically associate security and privacy attributes with [*Assignment: organization-defined subjects and objects*] in accordance with [*Assignment: organization-defined security and privacy policies*] as information is created and combined.

Supplemental Guidance: Dynamic association of security and privacy attributes is appropriate whenever the security or privacy characteristics of information changes over time. Attributes may change, for example, due to information aggregation issues (i.e., the security and privacy characteristics of individual information elements are different from the combined elements), changes in individual access authorizations (i.e., privileges), changes in the security category of information, and changes in security or privacy policies.

Related Controls: None.

(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.

Supplemental Guidance: The content or assigned values of security and privacy 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.

Related Controls: None.

(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*].

Supplemental Guidance: 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. Automated policy actions include, for example, retention date expirations, access control decisions, and information flow control decisions.

Related Controls: None.

(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).

Supplemental Guidance: The support provided by systems can include, for example, prompting users to select specific security or privacy attributes to be associated with specific information objects; employing automated mechanisms to categorize information with appropriate security or privacy attributes based on defined policies; or ensuring that the combination of selected security or privacy attributes selected is valid. Organizations consider the creation, deletion, or modification of security and privacy attributes when defining auditable events.

Related Controls: None.

(5) SECURITY AND PRIVACY ATTRIBUTES | ATTRIBUTE DISPLAYS FOR OUTPUT DEVICES

Display security and privacy attributes in human-readable form on each object that the system transmits to output devices to identify [*Assignment: organization-identified special dissemination, handling, or distribution instructions*] using [*Assignment: organization-identified human-readable, standard naming conventions*].

Supplemental Guidance: System outputs include, for example, pages, screens, or equivalent. System output devices include, for example, printers, notebook computers, video displays on ~~computer~~ workstations, and personal digital assistants. To mitigate the risk of unauthorized exposure of selected information, for example, shoulder surfing, the outputs display full attribute values when unmasked by the subscriber.

Related Controls: None.

(6) SECURITY AND PRIVACY ATTRIBUTES | MAINTENANCE OF ATTRIBUTE ASSOCIATION BY ORGANIZATION

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*].

Supplemental Guidance: This control enhancement requires individual users (as opposed to the system) to maintain associations of security and privacy attributes with subjects and objects.

Related Controls: None.

(7) SECURITY AND PRIVACY ATTRIBUTES | CONSISTENT ATTRIBUTE INTERPRETATION

Provide a consistent interpretation of security and privacy attributes transmitted between distributed system components.

Supplemental Guidance: To enforce security and privacy policies across multiple components in distributed systems ~~(e.g., distributed database management systems, cloud-based systems, and service-oriented architectures),~~ organizations provide a consistent interpretation of the attributes used in access enforcement and flow enforcement decisions. Organizations establish agreements and processes to ensure that all distributed system components implement security and privacy attributes with consistent interpretations in automated access and flow enforcement actions.

Related Controls: None.

(8) SECURITY AND PRIVACY ATTRIBUTES | ASSOCIATION TECHNIQUES AND TECHNOLOGIES

Implement [*Assignment: organization-defined techniques and technologies*] with [*Assignment: organization-defined level of assurance*] in associating security and privacy attributes to information.

Supplemental Guidance: The association (i.e., binding) of security and privacy attributes to information within systems is important for conducting automated access enforcement and flow enforcement actions. The association of such attributes can be accomplished with

technologies and techniques providing different levels of assurance. For example, systems can cryptographically bind attributes to information using digital signatures with the supporting cryptographic keys protected by hardware devices (sometimes known as hardware roots of trust).

(9) Related Controls: None.SECURITY AND PRIVACY ATTRIBUTES | ATTRIBUTE REASSIGNMENT

Reassign security and privacy attributes associated with information only via re-grading mechanisms validated using [*Assignment: organization-defined techniques or procedures*].

Supplemental Guidance: Validated re-grading mechanisms are employed by organizations to provide the requisite levels of assurance for security and privacy attribute reassignment activities. The validation is facilitated by ensuring that re-grading mechanisms are single purpose and of limited function. Since attribute reassignments can directly affect security and privacy policy enforcement actions ~~(e.g., access/flow enforcement decisions),~~, using trustworthy re-grading mechanisms is necessary to ensure that such mechanisms perform in a consistent and correct mode of operation.

Related Controls: None.

(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.

Supplemental Guidance: The content or assigned values of security and privacy 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 only.

Related Controls: None.

(11) SECURITY AND PRIVACY ATTRIBUTES | AUDIT CHANGES

Audit changes to security and privacy attributes.

Supplemental Guidance: None.

Related Controls: None.

References: FIPS Publications 140-2, 186-4; NIST Special Publications 800-162, 800-178.

AC-17 REMOTE ACCESS

Control:

a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and

b. Authorize remote access to the system prior to allowing such connections.

Supplemental Guidance: Remote access is access to organizational systems ~~by users~~ (or processes acting on behalf of users) communicating through external networks such as the Internet. Remote access methods include, for example, dial-up, broadband, and wireless. Organizations often employ encrypted virtual private networks (VPNs) to enhance confidentiality and integrity over remote connections. The use of encrypted VPNs ~~does not make the access non-remote; however, the use of VPNs, when adequately provisioned with appropriate security controls (e.g., employing appropriate encryption techniques for confidentiality and integrity protection) may provide~~provides sufficient assurance to the organization that it can effectively treat such connections as internal networks if the cryptographic mechanisms used are implemented in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines. Still, VPN connections traverse external networks, and the encrypted VPN does not enhance the availability of remote connections. VPNs with encrypted tunnels can also affect the capability to adequately monitor network communications traffic for malicious code. Remote access controls apply to systems other than public web servers or systems designed for public access. This control addresses authorization prior to allowing remote access without specifying the specific formats for such authorization. While organizations may use interconnection security

agreements to authorize remote access connections, such agreements are not required by this control. Enforcing access restrictions for remote connections is addressed in AC-3.

Related Controls: AC-2, AC-3, AC-4, AC-18, AC-19, AC-20, CM-10, IA-2, IA-3, IA-8, MA-4, PE-17, PL-2, PL-4, SC-10, SI-4.

Control Enhancements:

(1) REMOTE ACCESS | AUTOMATED MONITORING AND CONTROL

Monitor and control remote access methods.

Supplemental Guidance: Automated monitoring and control of remote access ~~sessions~~methods allows organizations to detect ~~cyber~~ attacks and ~~also~~ ensure ~~ongoing~~ compliance with remote access policies by auditing connection activities of remote users on a variety of system components including, for example, servers, workstations, notebook computers, smart phones, and tablets.

Related Controls: AU-2, AU-6, AU-12, AU-14.

(2) REMOTE ACCESS | PROTECTION OF CONFIDENTIALITY AND INTEGRITY USING ENCRYPTION

Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

Supplemental Guidance: The encryption strength of mechanism is selected based on the security categorization of the information.

Related Controls: SC-8, SC-12, SC-13.

(3) REMOTE ACCESS | MANAGED ACCESS CONTROL POINTS

Route all remote accesses through [*Assignment: organization-defined number*] managed network access control points.

Supplemental Guidance: Limiting the number of access control points for remote accesses reduces the attack surface for organizations. Organizations consider the Trusted Internet Connections initiative requirements for external network connections.

Related Controls: SC-7.

(4) REMOTE ACCESS | PRIVILEGED COMMANDS AND ACCESS

(a) Authorize the execution of privileged commands and access to security-relevant information via remote access only for [*Assignment: organization-defined needs*]; and

(b) Document the rationale for such access in the security plan for the system.

Supplemental Guidance: None.

Related Controls: AC-6.

(5) REMOTE ACCESS | MONITORING FOR UNAUTHORIZED CONNECTIONS

[Withdrawn: Incorporated into SI-4].

(6) REMOTE ACCESS | PROTECTION OF INFORMATION

Protect information about remote access mechanisms from unauthorized use and disclosure.

Supplemental Guidance: None.

Related Controls: AT-2, AT-3, PS-6.

(7) REMOTE ACCESS | ADDITIONAL PROTECTION FOR SECURITY FUNCTION ACCESS

[Withdrawn: Incorporated into AC-3(10)].

(8) REMOTE ACCESS | DISABLE NONSECURE NETWORK PROTOCOLS

[Withdrawn: Incorporated into CM-7].

(9) REMOTE ACCESS | DISCONNECT OR DISABLE ACCESS

Provide the capability to expeditiously disconnect or disable remote access to the system within [*Assignment: organization-defined time-period*].

Supplemental Guidance: This control enhancement requires organizations to have the capability to rapidly disconnect current users remotely accessing the system or disable further remote access. The speed of 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.

Related Controls: None.

References: NIST Special Publications 800-46, 800-77, 800-113, 800-114, 800-121; NIST Interagency Report 7966.

AC-18 WIRELESS ACCESS

Control:

a. Establish usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and

b. Authorize wireless access to the system prior to allowing such connections.

Supplemental Guidance: Wireless technologies include, for example, microwave, packet radio (ultra-high frequency/very high frequency), 802.11x, and Bluetooth. Wireless networks use authentication protocols ~~(e.g., EAP/TLS, PEAP),~~ which provide credential protection and mutual authentication.

Related Controls: 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.

Control Enhancements:

(1) WIRELESS ACCESS | AUTHENTICATION AND ENCRYPTION

Protect wireless access to the system using authentication of [*Selection (one or more): users; devices*] and encryption.

Supplemental Guidance: None.

Related Controls: SC-8, SC-13.

(2) WIRELESS ACCESS | MONITORING UNAUTHORIZED CONNECTIONS

[Withdrawn: Incorporated into SI-4].

(3) WIRELESS ACCESS | DISABLE WIRELESS NETWORKING

Disable, when not intended for use, wireless networking capabilities internally embedded within system components prior to issuance and deployment.

Supplemental Guidance: None.

Related Controls: None.

(4) WIRELESS ACCESS | RESTRICT CONFIGURATIONS BY USERS

Identify and explicitly authorize users allowed to independently configure wireless networking capabilities.

Supplemental Guidance: Organizational authorizations to allow selected users to configure wireless networking capability are enforced in part, by the access enforcement mechanisms employed within organizational systems.

Related Controls: SC-7, SC-15.

(5) WIRELESS ACCESS | ANTENNAS AND TRANSMISSION POWER LEVELS

Select radio antennas and calibrate transmission power levels to reduce the probability that signals from wireless access points can be received outside of organization-controlled boundaries.

Supplemental Guidance: Actions that may be taken by organizations to limit the unauthorized use of wireless communications outside of organization-controlled boundaries include, for example, reducing the power of wireless transmissions so that the transmissions are less likely to emit a signal that can be ~~used by adversaries~~captured outside of the physical perimeters of the organization; employing measures such as ~~TEMPEST~~emissions security to control wireless emanations; and using directional or beam forming antennas that reduce the likelihood that unintended receivers will be able to intercept signals. Prior to taking such mitigating actions, organizations can conduct periodic wireless surveys to understand the radio frequency profile of organizational systems as well as other systems that may be operating in the area.

Related Controls: PE-19.

References: NIST Special Publications 800-48, 800-94, 800-97.

AC-19 ACCESS CONTROL FOR MOBILE DEVICES

Control:

a. Establish usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices;

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

c. Protect and control mobile devices when outside of controlled areas.

Supplemental Guidance: 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, E-readers, and tablets. Mobile devices are typically associated with a single individual and the device is usually near the individual; however, the degree of proximity can vary depending upon on the form factor and size of the device. The processing, storage, and transmission capability of the mobile device may be comparable to or merely a subset of notebook/desktop systems, depending upon the nature and intended purpose of the device. Controlled areas are areas or spaces for which organizations provide sufficient physical or procedural safeguards to meet the requirements established for protecting information and systems.

Due to the large variety of mobile devices with different ~~technical~~ characteristics and capabilities, organizational restrictions may vary for the different classes/types of such devices. Usage restrictions and specific implementation guidance for mobile devices include, for example, configuration management, device identification and authentication, implementation of mandatory protective software ~~(e.g., malicious code detection, firewall),~~ scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware ~~(e.g., wireless, infrared). Organizations are cautioned that~~.

Usage restrictions and authorization to connect may vary among organizational systems. For example, the organization may authorize the connection of mobile devices to the organizational network and impose a set of usage restrictions while a system owner may withhold authorization for mobile device connection to specific applications or may impose additional usage restrictions before allowing mobile device connections to a system. The need to provide adequate security for mobile devices goes beyond the requirements in this control. Many safeguards for mobile devices are reflected in other security controls allocated to the initial control baselines as starting points for the development of security plans and overlays using the tailoring process. There may also be some overlap by the security controls within the different families of controls. AC-20 addresses mobile devices that are not organization-controlled.

Related Controls: AC-3, AC-4, AC-7, AC-17, AC-18, AC-20, CA-9, CM-2, CM-6, IA-3, MP-2, MP-4, MP-5, MP-7, PL-4, SC-7, SC-34, SC-43, SI-3, SI-4.

Control Enhancements:

(1) ACCESS CONTROL FOR MOBILE DEVICES | USE OF WRITABLE AND PORTABLE STORAGE DEVICES
[Withdrawn: Incorporated into MP-7].

(2) ACCESS CONTROL FOR MOBILE DEVICES | USE OF PERSONALLY OWNED PORTABLE STORAGE DEVICES
[Withdrawn: Incorporated into MP-7].

(3) ACCESS CONTROL FOR MOBILE DEVICES | USE OF PORTABLE STORAGE DEVICES WITH NO IDENTIFIABLE OWNER
[Withdrawn: Incorporated into MP-7].

(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*].

Supplemental Guidance: None.

Related Controls: CM-8, IR-4.

(5) ACCESS CONTROL FOR MOBILE DEVICES | FULL DEVICE AND CONTAINER-BASED ENCRYPTION

Employ [*Selection: full-device encryption; container encryption*] to protect the confidentiality and integrity of information on [*Assignment: organization-defined mobile devices*].

Supplemental Guidance: Container-based encryption provides a more fine-grained approach to the encryption of data/information on mobile devices, including, for example, encrypting selected data structures such as files, records, or fields.

Related Controls: SC-13, SC-28.

References: NIST Special Publications 800-114, 800-124, 800-164.

AC-20 USE OF EXTERNAL SYSTEMS

Control: Establish terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to:

a. Access the system from external systems; and

b. Process, store, or transmit organization-controlled information using external systems.

Supplemental Guidance: External systems are systems or components of systems that are outside of the authorization boundary established by organizations and for which organizations typically have no direct supervision and authority over the application of required security controls or the assessment of control effectiveness. External systems include, for example, personally owned systems, components, or devices ~~(e.g., notebook computers, smart phones, tablets, personal digital assistants)~~; privately owned computing and communications devices in commercial or public facilities ~~(e.g., hotels, train stations, convention centers, shopping malls, or airports);~~ ; systems owned or controlled by nonfederal organizations; and federal systems that are not owned by, operated by, or under the direct supervision and authority of the organization. This includes systems managed by contractors, systems owned by other federal agencies, and systems owned by other organizations~~.~~ within the same agency. This control addresses the use of external systems for the processing, storage, or transmission of organizational information, including, for example, accessing cloud services ~~(e.g., infrastructure as a service, platform as a service, or software as a service)~~ from organizational systems.

For some external systems (i.e., systems operated by other federal agencies and organizations subordinate to those agencies), the trust relationships that have been established between those organizations and the originating organization may be such, that no explicit terms and conditions are required. Systems within these organizations may not be considered external. These situations occur when, for example, there are pre-existing sharing and trust agreements (either implicit or explicit) established between federal agencies or organizations subordinate to those agencies, or

when such trust agreements are specified by applicable laws, Executive Orders, directives, regulations, or policies. Authorized individuals include, for example, 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 with regard to system access. Restrictions that organizations impose on authorized individuals need not be uniform, as those restrictions may vary depending on the trust relationships between organizations. Therefore, organizations may choose to impose different security restrictions on contractors than on state, local, or tribal governments.

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

Related Controls: AC-2, AC-3, AC-17, AC-19, CA-3, PL-2, PL-4, SA-9, SC-7.

Control Enhancements:

(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 required security and privacy controls on the external system as specified in the organization's security and privacy policies and security ~~plan~~and privacy plans; or

(b) Retention of approved system connection or processing agreements with the organizational entity hosting the external system.

Supplemental Guidance: This control enhancement recognizes that there are circumstances where individuals using external systems ~~(e.g., contractors, coalition partners)~~ need to access organizational systems. In those situations, organizations need confidence that the external systems contain the necessary security ~~safeguards (i.e., security~~ controls so as not to compromise, damage, or otherwise harm organizational systems. Verification that the required security controls have been implemented can be achieved, for example, by external, independent assessments, attestations, or other means, depending on the confidence level required by organizations.

Related Controls: CA-2.

(2) USE OF EXTERNAL SYSTEMS | PORTABLE STORAGE DEVICES

[Selection: Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems using the following [Assignment: organization-defined restrictions]; Prohibit the use of organization-controlled portable storage devices by authorized individuals on external systems].

Supplemental Guidance: Limits on the use of organization-controlled portable storage devices in external systems include, for example, complete prohibition of the use of such devices or restrictions on how the devices may be used and under what conditions the devices may be used.

Related Controls: MP-7, SC-41.

(3) USE OF EXTERNAL SYSTEMS | NON-ORGANIZATIONALLY OWNED SYSTEMS AND COMPONENTS ~~/ DEVICES~~

[Selection: Restrict the use of non-organizationally owned systems or system components~~, or devices~~ to process, store, or transmit organizational information using the following [Assignment: organization-defined restrictions]; Prohibit the use of non-organizationally owned systems or system components to process, store, or transmit organizational information].

Supplemental Guidance: Non-organizationally owned ~~devices~~systems or system components include ~~devices~~systems or system components owned by other organizations ~~(e.g., federal/state agencies, contractors)~~ and personally owned devices. There are potential risks to

using non-organizationally owned ~~devices.~~systems or system components. In some cases, the risk is sufficiently high as to prohibit such use. In other cases, ~~it~~the use of such systems or system components may be ~~such that the use of non-organizationally owned devices is~~ allowed but restricted in some way. Restrictions include, for example, requiring the implementation of approved security and privacy controls prior to authorizing ~~such connections;~~ the connection of non-organizationally owned systems and components; limiting access to certain types of information, services, or applications; using virtualization techniques to limit processing and storage activities to servers or other system components provisioned by the organization; and agreeing to the specified terms and conditions for usage. Organizations consult with the Office of the General Counsel regarding any legal issues associated with using personally owned devices ~~in operational environments~~, including, for example, requirements for conducting forensic analyses during investigations after an incident.

Related Controls: None.

(4) USE OF EXTERNAL SYSTEMS | NETWORK ACCESSIBLE STORAGE DEVICES

Prohibit the use of [*Assignment: organization-defined network accessible storage devices*] in external systems.

Supplemental Guidance: Network accessible storage devices in external systems include, for example, online storage devices in public, hybrid, or community cloud-based systems.

Related Controls: None.

References: FIPS Publication 199.

AC-21 INFORMATION SHARING

Control:

a. Facilitate information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions and privacy authorizations on the information 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.

Supplemental Guidance: This control applies to information that may be restricted in some manner based on some formal or administrative determination. Examples of such information include, contract-sensitive information, proprietary information, classified information related to special access programs or compartments, privileged medical information, and personally identifiable information. Risk analyses and privacy impact analyses can provide useful inputs to these determinations. Depending on the ~~particular~~ information-sharing circumstances, sharing partners may be defined at the individual, group, or organizational level. Information may be defined by content, type, security category, or special access program/compartment.

Related Controls: AC-3, AC-4, AC-16, SC-15.

Control Enhancements:

(1) INFORMATION SHARING | AUTOMATED DECISION SUPPORT

Enforce information-sharing decisions by authorized users based on access authorizations of sharing partners and access restrictions on information to be shared.

Supplemental Guidance: None.

Related Controls: None.

(2) INFORMATION SHARING | INFORMATION SEARCH AND RETRIEVAL

Implement information search and retrieval services that enforce [*Assignment: organization-defined information sharing restrictions*].

Supplemental Guidance: None.

Related Controls: None.

References: NIST Special Publication 800-150; NIST Interagency Report 8062.

AC-22 PUBLICLY ACCESSIBLE CONTENT

Control:

a. Designate individuals authorized to post information onto a publicly accessible system;

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.

Supplemental Guidance: In accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidelines, the public is not authorized access to nonpublic information including, for example, information protected under the Privacy Act and proprietary information. This control addresses systems that are controlled by the organization and accessible to the public, typically without identification or authentication. The posting of information on non-organization systems is covered by organizational policy.

Related Controls: AC-3, AT-2, AT-3, AU-13.

Control Enhancements: None.

References: None.

AC-23 DATA MINING PROTECTION

Control: Employ [*Assignment: organization-defined data mining prevention and detection techniques*] for [*Assignment: organization-defined data storage objects*] to ~~adequately~~ detect and protect against unauthorized data mining.

Supplemental Guidance: Data storage objects include, for example, databases, database records, and database fields. Data mining prevention and detection techniques include, for example, limiting the types of responses provided to database queries; limiting the number and the frequency of database queries to increase the work factor needed to determine the contents of such databases; and notifying organizational personnel when atypical database queries or accesses occur. This control focuses on the protection of organizational 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 now available as open source information residing on external sites, for example, through social networking or social media websites.

Related Controls: None.

Control Enhancements: None.

References: None.

AC-24 ACCESS CONTROL DECISIONS

Control: Establish procedures to ensure [*Assignment: organization-defined access control decisions*] are applied to each access request prior to access enforcement.

Supplemental Guidance: Access control decisions (also known as authorization decisions) occur when authorization information is applied to specific accesses. In contrast, access enforcement occurs when systems enforce access control decisions. While it is very common to have access control decisions and access enforcement implemented by the same entity, it is not required and it

is not always an optimal implementation choice. For some architectures and distributed systems, different entities may perform access control decisions and access enforcement.

Related Controls: AC-2, AC-3.

Control Enhancements:

(1) ACCESS CONTROL DECISIONS | TRANSMIT ACCESS AUTHORIZATION INFORMATION

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

Supplemental Guidance: In distributed systems, authorization processes and access control decisions may occur in separate parts of the systems. In such instances, authorization information is transmitted securely so timely access control decisions can be enforced at the appropriate locations. To support the access control decisions, it may be necessary to transmit as part of the access authorization information, supporting security attributes. This is because in distributed systems, there are various access control decisions that need to be made and different entities ~~(e.g., services)~~ make these decisions in a serial fashion, each requiring ~~some~~ security attributes to make the decisions. Protecting access authorization information ~~(i.e., access control decisions)~~ ensures that such information cannot be altered, spoofed, or ~~otherwise~~ compromised during transmission.

Related Controls: None.

(2) ACCESS CONTROL DECISIONS | NO USER OR PROCESS IDENTITY

Enforce access control decisions based on [*Assignment: organization-defined security attributes*] that do not include the identity of the user or process acting on behalf of the user.

Supplemental Guidance: 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.

Related Controls: None.

References: NIST Special Publications 800-162, 800-178.

AC-25 REFERENCE MONITOR

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

Supplemental Guidance: Information is represented internally within systems using abstractions known as data structures. Internal data structures can represent different types of entities, both active and passive. Active entities, also known as subjects, are associated with individuals, devices, or processes acting on behalf of individuals. Passive entities, also known as objects, are typically associated with data structures such as records, buffers, tables, files, inter-process pipes, and communications ports. Reference monitors enforce mandatory access control policies, a type of access control that restricts access to objects based on the identity of subjects or groups to which the subjects belong. The access controls are mandatory because subjects with certain privileges (i.e., access permissions) are restricted from passing those privileges on to any other subjects, either directly or indirectly—that is, the system strictly enforces the access control policy based on the rule set established by the policy. The tamperproof property of the reference monitor prevents adversaries from compromising the functioning of the mechanism. The always invoked property prevents adversaries from bypassing the mechanism and hence violating the security policy. The smallness property helps to ensure the completeness in the analysis and testing of the mechanism to detect weaknesses or deficiencies (i.e., latent flaws) that would prevent the enforcement of the security policy.

Related Controls: AC-3, AC-16, SC-3, SC-11, SC-39, SI-13.

Control Enhancements: None.

References: None.

3.2 AWARENESS AND TRAINING

Quick link to Awareness and Training summary table

AT-1 AWARENESS AND TRAINING POLICY AND PROCEDURES

Control:

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

1. A security and privacy 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

~~1.~~2. Procedures to facilitate the implementation of the security and privacy awareness and training policy and the associated security and privacy awareness and training controls;

b. Designate an [*Assignment: organization-defined senior management official*] to manage the security and privacy awareness and training policy and procedures;

~~b.~~c. Review and update the current security and privacy awareness and training:

1. Policy [*Assignment: organization-defined frequency*]; and

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

d. Ensure that the security and privacy awareness and training procedures implement the security and privacy awareness and training policy and controls; and

e. Develop, document, and implement remediation actions for violations of the awareness and training policy.

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of ~~selected security~~ the controls and control enhancements in the AT family. The risk management strategy is an important factor in establishing policy and procedures ~~reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards,~~. Comprehensive policy and ~~guidance.~~procedures help provide security and privacy assurance. Security and privacy program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general ~~information~~ security and privacy policy ~~for organizations or conversely,~~or can be represented by multiple policies reflecting the complex nature of ~~certain~~ organizations. The procedures can be established for ~~the~~ security ~~program in general~~and privacy programs and for ~~particular information~~ systems, if needed. ~~The~~Procedures describe how policies or controls are implemented and can be directed at the personnel 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. It is important to recognize that restating controls does not constitute an organizational ~~risk management strategy is a key factor in establishing~~ policy ~~and procedures.~~ or procedure.

Related Controls: PM-9, PS-8, SI-12.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-30, 800-39, 800-50, 800-100.

AT-2 ~~SECURITY~~ AWARENESS TRAINING

Control: Provide basic security and privacy awareness training to system users (including managers, senior executives, and contractors):

a. As part of initial training for new users;

b. When required by system changes; and

c. [*Assignment: organization-defined frequency*] thereafter.

Supplemental Guidance: Organizations determine the ~~appropriate~~ content of security and privacy awareness training and security and privacy awareness techniques based on the specific organizational requirements and the systems to which personnel have authorized access. The content includes ~~a basic~~an understanding of the need for information security and privacy and actions by users to maintain security and privacy and to respond to suspected security and privacy incidents. The content also addresses an awareness of the need for operations security. Security and privacy awareness techniques can include, for example, displaying posters, offering supplies inscribed with security and privacy reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting information security and privacy awareness events. Awareness training after the initial training (i.e., described AT-2c) is conducted at a minimum frequency consistent with applicable laws, directives, regulations, and policies. Such 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, and/or a subset of topics from the initial training.

Related Controls: AC-17, AC-22, AT-3, AT-4, CP-3, IA-4, IR-2, IR-7, IR-9, PA-2, PL-4, PM-13, PM-22, PS-7, SA-16.

Control Enhancements:

(1) ~~*SECURITY*~~ AWARENESS TRAINING | PRACTICAL EXERCISES

Include practical exercises in ~~security~~ awareness training that simulate ~~actual cyber attacks~~security and privacy incidents.

Supplemental Guidance: Practical exercises may include, for example, no-notice social engineering attempts to collect information, gain unauthorized access, or simulate the adverse impact of opening malicious email attachments or invoking, via spear phishing attacks, malicious web links. Privacy-related practical exercises may include, for example, practice modules with quizzes on handling personally identifiable information and affected individuals in various scenarios.

Related Controls: CA-2, CA-7, CP-4, IR-3.

(2) AWARENESS TRAINING | INSIDER THREAT

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

Supplemental Guidance: Potential indicators and possible precursors of insider threat can include behaviors such as inordinate, long-term job dissatisfaction, attempts to gain access to information not required for job performance, unexplained access to financial resources, bullying or sexual harassment of fellow employees, workplace violence, and other serious violations of organizational policies, procedures, directives, rules, or practices. Security and privacy awareness training includes how to communicate the concerns of employees and management regarding potential indicators of insider threat through ~~appropriate~~ organizational channels in accordance with established policies and procedures.

Related Controls: PM-12.

(3) AWARENESS TRAINING | SOCIAL ENGINEERING AND MINING

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

Supplemental Guidance: Social engineering is an attempt to trick someone into revealing information or taking an action that can be used to attack or compromise systems. Examples of social engineering include phishing, pretexting, baiting, quid pro quo, and tailgaiting. Social mining is an attempt, in a social setting, to gather information about the organization that may support future attacks. Security and privacy awareness training includes information on how to communicate concerns of employees and management regarding potential and

actual instances of social engineering and mining through organizational channels based on established policies and procedures.

Related Controls: None.

References: NIST Special Publication 800-50.

AT-3 ROLE-BASED ~~SECURITY~~ TRAINING

Control: Provide role-based security and privacy training to personnel with ~~assigned security~~the following roles and responsibilities: [*Assignment: organization-defined roles and responsibilities*]:

a. Before authorizing access to the system or performing assigned duties;

b. When required by system changes; and

c. [*Assignment: organization-defined frequency*] thereafter.

Supplemental Guidance: Organizations determine the appropriate content of security and privacy training based on the assigned roles and responsibilities of individuals and the specific security and privacy requirements of organizations and the systems to which personnel have authorized access~~. In addition, organizations provide~~, including security-related technical training specifically tailored for assigned duties. Roles that may require role-based security and privacy training include, for example, system owners; authorizing officials; system security officers; privacy officers; enterprise architects~~, information system developers,~~; acquisition and procurement officials; systems engineers; system ~~managers,~~and software developers; system, network, and database administrators; personnel conducting configuration management ~~and auditing~~ activities; personnel performing ~~independent~~ verification and validation activities~~, security control assessors, and other~~; auditors; personnel having access to system-level software~~, adequate security-related technical training specifically tailored for their assigned duties.~~; security and privacy control assessors; personnel with contingency planning and incident response duties; personnel with privacy management responsibilities; and personnel having access to personally identifiable information. Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards and countermeasures. Such training can include, for example, policies, procedures, tools, 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 security within the context of organizational information security and privacy programs. Role-based security and privacy training also applies to contractors providing services to federal agencies.

Related Controls: AC-17, AC-22, AT-2, AT-4, CP-3, IR-2, IR-7, IR-9, IR-10, PL-4, PM-13, PM-24, PS-7, SA-3, SA-11, SA-12, SA-16, SA-19.

Control Enhancements:

(1) ~~SECURITY~~ROLE-BASED TRAINING | ENVIRONMENTAL CONTROLS

Provide [*Assignment: organization-defined personnel or roles*] with initial and [*Assignment: organization-defined frequency*] training in the employment and operation of environmental controls.

Supplemental Guidance: Environmental controls include, for example, fire suppression and detection devices/systems, sprinkler systems, handheld fire extinguishers, fixed fire hoses, smoke detectors, temperature/humidity, heating, ventilation, and air conditioning, and power within the facility. Organizations identify personnel with specific roles and responsibilities associated with environmental controls requiring specialized training.

Related Controls: PE-1, PE-11, PE-13, PE-14, PE-15.

(2) ROLE-BASED TRAINING | PHYSICAL SECURITY CONTROLS

Provide [*Assignment: organization-defined personnel or roles*] with initial and [*Assignment: organization-defined frequency*] training in the employment and operation of physical security controls.

Supplemental Guidance: Physical security controls include, for example, physical access control devices, physical intrusion alarms, monitoring/surveillance equipment, and security guards (deployment and operating procedures). Organizations identify personnel with specific roles and responsibilities associated with physical security controls requiring specialized training.

Related Controls: PE-2, PE-3, PE-4.

(3) ROLE-BASED TRAINING | PRACTICAL EXERCISES

~~The organization includes~~Include practical exercises in security and privacy training that reinforce training objectives.

Supplemental Guidance: Practical exercises for security may include, for example, security training for software developers that includes simulated cyber-attacks exploiting common software vulnerabilities ~~(e.g., buffer overflows),~~ or spear/whale phishing attacks targeted at senior leaders/executives. ~~These types of~~ Practical exercises ~~help developers better understand the effects of such vulnerabilities and appreciate the need for security coding standards~~for privacy may include, for example, practice modules with quizzes on handling personally identifiable information in various scenarios, and ~~processes~~model scenarios on conducting privacy impact assessments.

Related Controls: None.

(4) ROLE-BASED TRAINING | SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR

Provide training to personnel on [*Assignment: organization-defined indicators of malicious code*] to recognize suspicious communications and anomalous behavior in organizational systems.

Supplemental Guidance: A well-trained workforce provides another organizational safeguard that can be employed as part of a defense-in-depth strategy to protect organizations against malicious code coming in to organizations via email or the web applications. Personnel are trained to look for indications of potentially suspicious email for example, receiving an unexpected email, receiving an email containing strange or poor grammar, or receiving an email from an unfamiliar sender but who appears to be from a known sponsor or contractor. Personnel are also trained on how to respond to suspicious email or web communications ~~(e.g., not opening attachments, not clicking on embedded web links, and checking the source of email addresses).~~ For this process to work effectively, organizational personnel are trained and made aware of what constitutes suspicious communications. Training personnel on how to recognize anomalous behaviors in organizational systems can potentially provide early warning for the presence of malicious code. Recognition of such anomalous behavior by organizational personnel can supplement automated malicious code detection and protection tools and systems employed by organizations.

Related Controls: None.

(5) ROLE-BASED TRAINING | PERSONALLY IDENTIFIABLE INFORMATION PROCESSING

Provide personnel who process personally identifiable information with initial and [*Assignment: organization-defined frequency*] training on:

(a) Organizational authority for collecting personally identifiable information;

(b) Authorized uses of personally identifiable information;

(c) Content of System of Records Notices;

(d) Authorized sharing of personally identifiable information with external parties; and

(e) Consequences of unauthorized use or sharing of personally identifiable information.

Supplemental Guidance: Role-based training on handling personally identifiable information helps prevent unauthorized collections or uses of personally identifiable information.

Related Controls: PA-3, PA-4.

References: NIST Special Publication 800-50.

AT-4 ~~SECURITY~~ TRAINING RECORDS

Control:

a. Document and monitor individual system security and privacy training activities including basic security and privacy awareness training and specific role-based system security and privacy training; and

b. Retain individual training records for [*Assignment: organization-defined time-period*].

Supplemental Guidance: Documentation for specialized training may be maintained by individual supervisors at the option of the organization. The National Archives and Records Administration provides guidance on records retention.

Related Controls: AT-2, AT-3, CP-3, IR-2, PM-14, SI-12.

Control Enhancements: None.

References: None.

AT-5 CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS

[Withdrawn: Incorporated into PM-15].

3.3 AUDIT AND ACCOUNTABILITY

Quick link to Audit and Accountability summary table

AU-1 AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES

Control:

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

1. An 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 senior management official*] to manage the audit and accountability policy and procedures;

~~b.~~c. Review and update the current audit and accountability:

1. Policy [*Assignment: organization-defined frequency*]; and

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

d. Ensure that the audit and accountability procedures implement the audit and accountability policy and controls; and

e. Develop, document, and implement remediation actions for violations of the audit and accountability policy.

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of ~~selected security~~ the controls and control enhancements in the AU family. The risk management strategy is an important factor in establishing policy and procedures ~~reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards,~~. Comprehensive policy and ~~guidance~~procedures help provide security and privacy assurance. Security and privacy program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general security and privacy policy ~~for organizations or conversely,~~or can be represented by multiple policies reflecting the complex nature of ~~certain~~ organizations. The procedures can be established for ~~the~~ security ~~program in general~~and privacy programs and for ~~particular information~~ systems, if needed. ~~The~~Procedures describe how policies or controls are implemented and can be directed at the personnel 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. It is important to recognize that restating controls does not constitute an organizational ~~risk management strategy is a key factor in establishing~~ policy ~~and procedures.~~ or procedure.

Related Controls: PM-9, PS-8, SI-12.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-30, 800-39, 800-50, 800-100.

AU-2 AUDIT EVENTS

Control:

a. ~~Determines~~Verify that the ~~information~~ system ~~is capable of auditing~~can audit the following ~~events~~event types: [*Assignment: organization-defined auditable ~~events~~event types*];

b. Coordinate the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable ~~events~~event types;

c. Provide a rationale for why the auditable ~~events~~event types are deemed to be adequate to support after-the-fact investigations of security and privacy incidents; and

d. ~~Determines~~Specify that the following ~~events~~event types are to be audited within the ~~information~~ system: [*Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event*].

Supplemental Guidance: An event is any observable occurrence in an organizational system. Organizations identify audit ~~events~~event types as those events which are significant and relevant to the security of systems and the environments in which those systems operate to meet specific and ongoing audit needs. Audit ~~events~~event types can include, for example, password changes; failed logons or failed accesses related to systems; security attribute changes, administrative privilege usage, PIV credential usage, ~~or third-party~~query parameters, or external credential usage. In determining the set of auditable ~~events~~event types, organizations consider the auditing appropriate for each of the security controls to be implemented. To balance auditing requirements with other system needs, this control also requires identifying that subset of *auditable* ~~events~~event types that are *audited* at a given point in time. For example, organizations may determine that systems must have the capability to log every file access both successful and unsuccessful, but not activate that capability except for specific circumstances due to the potential burden on system performance.

Auditing requirements, including the need for auditable events, may be referenced in other security and privacy controls and control enhancements~~.~~ for example, AC-2(4), AC-3(10), AC-6(9), AC-16(11), AC-17(1), CM-3.f, CM-5(1), IA-3(3.b), MA-4(1), MP-4(2), PA-4.d, PE-3, PM-22, RA-8, SC-7(9), SC-7(15), SI-3(8), SI-4(22), SI-7(8), and SI-10(1). Organizations also include auditable ~~events~~event types that are required by applicable ~~federal~~ laws, Executive Orders, directives, policies, regulations, standards, and guidelines. Audit records can be generated at various levels ~~of abstraction~~, including at the packet level as information traverses the network. Selecting the appropriate level of ~~abstraction~~auditing is an important aspect of an audit capability and can facilitate the identification of root causes to problems. Organizations consider in the definition of auditable ~~events~~event types, the auditing necessary to cover related ~~events~~event types such as the steps in distributed, transaction-based processes ~~(e.g., processes that are distributed across multiple organizations)~~ and actions that occur in service-oriented architectures.

Related Controls: 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, IA-3, MA-4, MP-4, PA-4, PE-3, PM-22, RA-8, SC-7, SC-18, SI-3, SI-4, SI-7, SI-10, SI-11.

Control Enhancements:

(1) AUDIT EVENTS | COMPILATION OF AUDIT RECORDS FROM MULTIPLE SOURCES

[Withdrawn: Incorporated into AU-12].

(2) AUDIT EVENTS | SELECTION OF AUDIT EVENTS BY COMPONENT

[Withdrawn: Incorporated into AU-12].

(3) AUDIT EVENTS | REVIEWS AND UPDATES

Review and update the audited events [*Assignment: organization-defined frequency*].

Supplemental Guidance: Over time, the events that organizations believe should be audited may change. Reviewing and updating the set of audited events periodically is necessary to ensure that the current set is still necessary and sufficient.

Related Controls: None.

(4) AUDIT EVENTS | PRIVILEGED FUNCTIONS

[Withdrawn: Incorporated into AC-6(9)].

References: NIST Special Publication 800-92.

AU-3 CONTENT OF AUDIT RECORDS

Control: The system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

Supplemental Guidance: Audit record content that may be necessary to satisfy the requirement of this control, includes, for example, time stamps, source and destination addresses, user or process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked. Event outcomes can include indicators of event success or failure and event-specific results, for example, the security and privacy state of the system after the event occurred.

Related Controls: AU-2, AU-8, AU-12, AU-14, MA-4, SI-7, SI-11.

Control Enhancements:

(1) CONTENT OF AUDIT RECORDS | ADDITIONAL AUDIT INFORMATION

Generate audit records containing the following additional information: [*Assignment: organization-defined additional, more detailed information*].

Supplemental Guidance: Implementation of this control enhancement is dependent on system functionality to configure audit record content. Detailed information that organizations may consider in audit records includes, for example, full text recording of privileged commands or the individual identities of group account users. Organizations consider limiting the additional audit information to only that information explicitly needed for specific audit requirements. This facilitates the use of audit trails and audit logs by not including information that could potentially be misleading or could make it more difficult to locate information of interest.

Related Controls: None.

(2) CONTENT OF AUDIT RECORDS | CENTRALIZED MANAGEMENT OF PLANNED AUDIT RECORD CONTENT

Provide centralized management and configuration of the content to be captured in audit records generated by [*Assignment: organization-defined system components*].

Supplemental Guidance: This control enhancement requires that the content to be captured in audit records be configured from a central location (necessitating automation). Organizations coordinate the selection of required audit content to support the centralized management and configuration capability provided by the system.

Related Controls: AU-6, AU-7.

(3) CONTENT OF AUDIT RECORDS | LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS

Limit personally identifiable information contained in audit records to the following elements identified in the privacy risk assessment: [*Assignment: organization-defined elements*].

Supplemental Guidance: Limiting personally identifiable information in audit records when such information is not needed for operational purposes helps reduce the level of privacy risk created by a system.

Related Controls: None.

References: NIST Interagency Report 8062.

AU-4 AUDIT STORAGE CAPACITY

Control: Allocate audit record storage capacity ~~in accordance with~~to accommodate [*Assignment: organization-defined audit record ~~storage~~retention requirements*].

Supplemental Guidance: Organizations consider the types of auditing to be performed and the audit processing requirements when allocating audit storage capacity. Allocating sufficient audit storage

capacity reduces the likelihood of such capacity being exceeded and resulting in the potential loss or reduction of auditing capability.

Related Controls: AU-2, AU-5, AU-6, AU-7, AU-9, AU-11, AU-12, AU-14, SI-4.

Control Enhancements:

(1) AUDIT STORAGE CAPACITY | TRANSFER TO ALTERNATE STORAGE

Off-load audit records [*Assignment: organization-defined frequency*] onto a different system or media than the system being audited.

Supplemental Guidance: Off-loading is a process designed to preserve the confidentiality and integrity of audit records by moving the records from the primary system to a secondary or alternate system. It is a common process in systems with limited audit storage capacity; the audit storage is used only in a transitory fashion until the system can communicate with the secondary or alternate system designated for storing the audit records, at which point the information is transferred.

Related Controls: None.

References: None.

AU-5 RESPONSE TO AUDIT PROCESSING FAILURES

Control:

a. Alert [*Assignment: organization-defined personnel or roles*] in the event of an audit processing failure within [*Assignment: organization-defined time-period*]; and

b. Take the following additional actions: [*Assignment: organization-defined actions to be taken*].

Supplemental Guidance: Organization-defined actions include, for example, shutting down the system; overwriting oldest audit records; and stopping the generation of audit recordsExamples of audit processing failures include software and hardware errors; failures in the audit capturing mechanisms; and audit storage capacity being reached or exceeded. Organizations may choose to define additional actions for ~~different~~ audit processing failures based on the type of failure, the location of the failure, the severity of the failure, or a combination of such factors. This control applies to each audit data storage repository (i.e., distinct system component where audit records are stored), the total audit storage capacity of organizations (i.e., all audit data storage repositories combined), or both.

Related Controls: AU-2, AU-4, AU-7, AU-9, AU-11, AU-12, AU-14, SI-4, SI-12.

Control Enhancements:

(1) RESPONSE TO AUDIT PROCESSING FAILURES | AUDIT STORAGE CAPACITY

Provide a warning to [*Assignment: organization-defined personnel, roles, and/or locations*] within [*Assignment: organization-defined time-period*] when allocated audit record storage volume reaches [*Assignment: organization-defined percentage*] of repository maximum audit record storage capacity.

Supplemental Guidance: Organizations may have multiple audit data storage repositories distributed across multiple system components, with each repository having different storage volume capacities.

Related Controls: None.

(2) RESPONSE TO AUDIT PROCESSING FAILURES | REAL-TIME ALERTS

Provide an alert in [*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 failure events requiring real-time alerts*].

Supplemental Guidance: 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).

Related Controls: None.

(3) RESPONSE TO AUDIT PROCESSING FAILURES | CONFIGURABLE TRAFFIC VOLUME THRESHOLDS

Enforce configurable network communications traffic volume thresholds reflecting limits on auditing capacity and [*Selection: rejects; delays*] network traffic above those thresholds.

Supplemental Guidance: Organizations have the capability to reject or delay the processing of network communications traffic if auditing such traffic is determined to exceed the storage capacity of the system audit function. The rejection or delay response is triggered by the established organizational traffic volume thresholds which can be adjusted based on changes to audit storage capacity.

Related Controls: None.

(4) RESPONSE TO AUDIT PROCESSING FAILURES | SHUTDOWN ON FAILURE

Invoke a [*Selection: full system shutdown; partial system shutdown; degraded operational mode with limited mission/business functionality available*] in the event of [*Assignment: organization-defined audit failures*], unless an alternate audit capability exists.

Supplemental Guidance: Organizations determine the types of audit failures that can trigger automatic system shutdowns or degraded operations. Because of the importance of ensuring mission and business continuity, organizations may determine that the nature of the audit failure is not so severe that it warrants a complete shutdown of the system supporting the core organizational missions and business operations. In those instances, partial system shutdowns or operating in a degraded mode with reduced capability may be viable alternatives.

Related Controls: AU-15.

References: None.

AU-6 AUDIT REVIEW, ANALYSIS, AND REPORTING

Control:

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

b. Report findings to [*Assignment: organization-defined personnel or roles*]; and

c. Adjust the level of audit 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.

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

Related Controls: AC-2, AC-3, AC-6, AC-7, AC-17, AU-7, AU-16, 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, SC-7, SI-3, SI-4, SI-7.

Control Enhancements:

(1) AUDIT REVIEW, ANALYSIS, AND REPORTING | AUTOMATED PROCESS INTEGRATION

Employ automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.

Supplemental Guidance: Organizational processes benefiting from integrated audit review, analysis, and reporting include, for example, incident response, continuous monitoring, contingency planning, and Inspector General audits.

Related Controls: PM-7.

(2) AUDIT REVIEW, ANALYSIS, AND REPORTING | AUTOMATED SECURITY ALERTS

[Withdrawn: Incorporated into SI-4].

(3) AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATE AUDIT REPOSITORIES

Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.

Supplemental Guidance: Organization-wide situational awareness includes awareness across all three tiers of risk management (i.e., organizational, mission/business process, and system) and supports cross-organization awareness.

Related Controls: AU-12, IR-4.

(4) AUDIT REVIEW, ANALYSIS, AND REPORTING | CENTRAL REVIEW AND ANALYSIS

Provide and implement the capability to centrally review and analyze audit records from multiple components within the system.

Supplemental Guidance: Automated mechanisms for centralized reviews and analyses include, for example, Security Information Management products.

Related Controls: AU-2, AU-12.

(5) AUDIT REVIEW, ANALYSIS, AND REPORTING | ~~*INTEGRATION / SCANNING AND MONITORING CAPABILITIES*~~ INTEGRATED ANALYSIS OF AUDIT RECORDS

Integrate analysis of audit records with analysis of [*Selection (one or more): vulnerability scanning information; performance data; system monitoring information;* [*Assignment: organization-defined data/information collected from other sources*]] to further enhance the ability to identify inappropriate or unusual activity.

Supplemental Guidance: This control enhancement does not require vulnerability scanning, the generation of performance data, or system monitoring. Rather, the enhancement requires that the analysis of information being otherwise produced in these areas is integrated with the analysis of audit information. Security Event and Information Management System tools can facilitate audit record aggregation/consolidation from multiple system components as well as audit record correlation and analysis. The use of standardized audit record analysis scripts developed by organizations (with localized script adjustments, as necessary) provides more cost-effective approaches for analyzing audit record information collected. The correlation of audit record information with vulnerability scanning information is important in determining the veracity of vulnerability scans and correlating attack detection events with scanning results. Correlation with performance data can ~~help~~ uncover denial of service attacks or ~~cyber~~other types of attacks resulting in unauthorized use of resources. Correlation with system monitoring information can assist in uncovering attacks and in better relating audit information to operational situations.

Related Controls: AU-12, IR-4.

(6) AUDIT 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.

Supplemental Guidance: The correlation of physical audit information and audit logs from systems may assist organizations in identifying examples of 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.

Related Controls: None.

(7) AUDIT 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 information.

Supplemental Guidance: Organizations specify permitted actions for system processes, roles, and/or users associated with the review, analysis, and reporting of audit records through account management techniques. Specifying permitted actions on audit information is a way to enforce the principle of least privilege. Permitted actions are enforced by the system and include, for example, read, write, execute, append, and delete.

Related Controls: None.

(8) AUDIT REVIEW, ANALYSIS, AND REPORTING | FULL TEXT ANALYSIS OF PRIVILEGED COMMANDS

Perform a full text analysis of audited privileged commands in a physically distinct component or subsystem of the system, or other system that is dedicated to that analysis.

Supplemental Guidance: This control enhancement requires a distinct environment for the dedicated analysis of audit information related to privileged users without compromising such information on the system where the users have elevated privileges including the capability to execute privileged commands. Full text analysis refers to analysis that considers the full text of privileged commands (i.e., commands and all parameters) as opposed to analysis that considers only the name of the command. Full text analysis includes, for example, the use of pattern matching and heuristics.

Related Controls: AU-3, AU-9, AU-11, AU-12.

(9) AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATION WITH INFORMATION FROM NONTECHNICAL SOURCES

Correlate information from nontechnical sources with audit information to enhance organization-wide situational awareness.

Supplemental Guidance: Nontechnical sources include, for example, human resources records documenting organizational policy violations including, for example, sexual harassment incidents and improper use of organizational information assets. Such information can lead to a more directed analytical effort to detect potential malicious insider activity. Due to the sensitive nature of the information available from nontechnical sources, organizations limit access to such information to minimize the potential for the inadvertent release of privacy-related information to individuals that do not have a need to know. Thus, correlation of information from nontechnical sources with audit information generally occurs only when individuals are suspected of being involved in a security incident. Organizations obtain legal advice prior to initiating such actions.

Related Controls: PM-12.

(10) AUDIT REVIEW, ANALYSIS, AND REPORTING | AUDIT LEVEL ADJUSTMENT

~~**The organization adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.**~~

[Withdrawn: Incorporated into AU-6]. ~~Supplemental Guidance:~~

~~The frequency, scope, and/or depth of the audit review, analysis, and reporting may be adjusted to meet organizational needs based on new information received.~~References: NIST Special Publications 800-86, 800-101.

AU-7 AUDIT REDUCTION AND REPORT GENERATION

Control: Provide and implement an audit reduction and report generation capability that:

a. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and

b. Does not alter the original content or time ordering of audit records.

Supplemental Guidance: Audit reduction is a process that manipulates collected audit information and organizes such information in a summary format that is more meaningful to analysts. Audit reduction and report generation capabilities do not always emanate from the same system or from the same organizational entities conducting auditing activities. Audit reduction capability can

include, for example, modern data mining techniques with advanced data filters to identify anomalous behavior in audit records. The report generation capability provided by the system can generate customizable reports. Time ordering of audit records can be a significant issue if the granularity of the timestamp in the record is insufficient.

Related Controls: 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.

Control Enhancements:

(1) AUDIT REDUCTION AND REPORT GENERATION | AUTOMATIC PROCESSING

Provide and implement the capability to process audit records for events of interest based on [*Assignment: organization-defined audit fields within audit records*].

Supplemental Guidance: Events of interest can be identified by the content of specific audit record fields including, for example, identities of individuals, event types, event locations, event times, event dates, system resources involved, Internet Protocol addresses involved, or information objects accessed. Organizations may define audit event criteria to any degree of granularity required, for example, locations selectable by general networking location or selectable by specific system component.

Related Controls: None.

(2) AUDIT REDUCTION AND REPORT GENERATION | AUTOMATIC SORT AND SEARCH

Provide and implement the capability to sort and search audit records for events of interest based on the content of [*Assignment: organization-defined audit fields within audit records*].

Supplemental Guidance: Sorting and searching of audit records may be based upon the contents of audit record fields, for example, date and time of events; user identifiers; Internet Protocol addresses involved in the event; type of event; or event success or failure.

Related Controls: None.

References: None.

AU-8 TIME STAMPS

Control:

a. Use internal system clocks to generate time stamps for audit records; and

b. Record time stamps for audit records that can be mapped to Coordinated Universal Time or Greenwich Mean Time and meets [*Assignment: organization-defined granularity of time measurement*].

Supplemental Guidance: Time stamps generated by the system include date and time. Time is commonly expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC. Granularity of time measurements refers to the degree of synchronization between system clocks and reference clocks, for example, clocks synchronizing within hundreds of milliseconds or tens of milliseconds. Organizations may define different time granularities for different system components. Time service can also be critical to other security capabilities such as access control and identification and authentication, depending on the nature of the mechanisms used to support those capabilities.

Related Controls: AU-3, AU-12, AU-14.

Control Enhancements:

(1) TIME STAMPS | 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*].

Supplemental Guidance: This control enhancement provides uniformity of time stamps for systems with multiple system clocks and systems connected over a network.

Related Controls: None.

(2) TIME STAMPS | SECONDARY AUTHORITATIVE TIME SOURCE

(a) Identify a secondary authoritative time source that is ~~located~~ 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.

Supplemental Guidance: It may be necessary to employ geolocation information to determine that the secondary authoritative time source is in a different geographic region.

Related Controls: None.

References: None.

AU-9 PROTECTION OF AUDIT INFORMATION

Control: Protect audit information and audit tools from unauthorized access, modification, and deletion.

Supplemental Guidance: Audit information includes all information, for example, audit records, audit settings, audit reports, and personally identifiable information, needed to successfully audit system activity. This control focuses on technical or automated protection of audit information. Physical protection of audit information is addressed by media protection controls and physical and environmental protection controls.

Related Controls: AC-3, AC-6, AU-6, AU-11, AU-14, AU-15, MP-2, MP-4, PE-2, PE-3, PE-6, SC-8, SI-4.

Control Enhancements:

(1) PROTECTION OF AUDIT INFORMATION | HARDWARE WRITE-ONCE MEDIA

Write audit trails to hardware-enforced, write-once media.

Supplemental Guidance: This control enhancement applies to the initial generation of audit trails (i.e., the collection of audit records that represents the audit information to be used for detection, analysis, and reporting purposes) and to the backup of those audit trails. The enhancement does not apply to the initial generation of audit records prior to being written to an audit trail. Write-once, read-many (WORM) media includes, for example, Compact Disk-Recordable (CD-R) and Digital Video Disk-Recordable (DVD-R). In contrast, the use of switchable write-protection media such as on tape cartridges or Universal Serial Bus (USB) drives results in write-protected, but not write-once, media.

Related Controls: AU-4, AU-5.

(2) PROTECTION OF AUDIT INFORMATION | ~~*AUDIT BACKUP*~~STORE ON SEPARATE PHYSICAL SYSTEMS OR COMPONENTS

~~backs up~~Store audit records [*Assignment: organization-defined frequency*] ~~onto~~in a repository that is part of a physically different system or system component than the system or component being audited.

Supplemental Guidance: ~~This control enhancement~~ Storing audit information in a repository separate from the audited system or system component helps to ensure that a compromise of the ~~information~~ system being audited does not also result in a compromise of the audit records. It may also enable management of audit records as an organization-wide activity. This control enhancement applies to initial generation as well as backup or long-term storage of audit information.

Related Controls: AU-4, AU-5.

(3) PROTECTION OF AUDIT INFORMATION | CRYPTOGRAPHIC PROTECTION

Implement cryptographic mechanisms to protect the integrity of audit information and audit tools.

Supplemental Guidance: Cryptographic mechanisms used for protecting the integrity of audit information include, for example, signed hash functions using asymmetric cryptography

enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the secret key used to generate the hash.

Related Controls: AU-10, SC-12, SC-13.

(4) PROTECTION OF AUDIT INFORMATION | ACCESS BY SUBSET OF PRIVILEGED USERS

Authorize access to management of audit functionality to only [*Assignment: organization-defined subset of privileged users*].

Supplemental Guidance: Individuals with privileged access to a system and who are also the subject of an audit by that system, may affect the reliability of audit information by inhibiting audit activities or modifying audit records. This control enhancement requires that privileged access be further defined between audit-related privileges and other privileges, thus limiting the users with audit-related privileges.

Related Controls: AC-5.

(5) PROTECTION OF AUDIT INFORMATION | DUAL AUTHORIZATION

Enforce dual authorization for [*Selection (one or more): movement; deletion*] of [*Assignment: organization-defined audit information*].

Supplemental Guidance: Organizations may choose different selection options for different types of audit information. Dual authorization mechanisms require the approval of two authorized individuals to execute. Dual authorization may also be known as two-person control.

Related Controls: AC-3.

(6) PROTECTION OF AUDIT INFORMATION | READ ONLY ACCESS

Authorize read-only access to audit information to [*Assignment: organization-defined subset of privileged users*].

Supplemental Guidance: Restricting privileged user authorizations to read-only helps to limit the potential damage to organizations that could be initiated by such users, for example, deleting audit records to cover up malicious activity.

Related Controls: None.

(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 component being audited.

Supplemental Guidance: This control enhancement helps reduce the risk of a vulnerability specific to an operating system resulting in a compromise of the audit records.

Related controls: AU-4, AU-5, AU-11, SC-29.

References: FIPS Publications 140-2, 180-4, 202.

AU-10 NON-REPUDIATION

Control: Protect against an individual (or process acting on behalf of an individual) falsely denying having performed [*Assignment: organization-defined actions to be covered by non-repudiation*].

Supplemental Guidance: Types of individual actions covered by non-repudiation include creating information, sending and receiving messages, and approving information ~~(e.g., indicating concurrence or signing a contract).~~ Non-repudiation protects individuals against later claims by authors of not having authored ~~particular~~certain documents; senders of not having transmitted messages; receivers of not having received messages; and individual signatories of not having signed documents. Non-repudiation services can be used to determine if information originated from a certain individual, or if an individual took specific actions, for example, sending an email, signing a contract, or approving a procurement request, or received specific information. Organizations obtain non-repudiation services by employing various techniques or mechanisms including, for example, digital signatures and digital message receipts.

Related Controls: AU-9, PM-12, SC-8, SC-12, SC-13, SC-16, SC-17, SC-23.

Control Enhancements:

(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.

Supplemental Guidance: This control enhancement supports audit requirements that provide organizational personnel with the means to identify who produced specific information in the event of an information transfer. Organizations determine and approve the strength of the binding between the information producer and the information based on the security category of the information and relevant risk factors.

Related Controls: AC-4, AC-16.

(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.

Supplemental Guidance: This control enhancement prevents the modification of information between production and review. The validation of bindings can be achieved, for example, using cryptographic checksums. Organizations determine if validations are in response to user requests or generated automatically.

Related Controls: AC-3, AC-4, AC-16.

(3) NON-REPUDIATION | CHAIN OF CUSTODY

Maintain reviewer or releaser identity and credentials within the established chain of custody for all information reviewed or released.

Supplemental Guidance: Chain of custody is a process that tracks the movement of evidence through its collection, safeguarding, and analysis life cycle by documenting each person who handled the evidence, the date and time it was collected or transferred, and the purpose for the transfer. If the reviewer is a human or if the review function is automated but separate from the release/transfer function, the system associates the identity of the reviewer of the information to be released with the information and the information label. In the case of human reviews, this control enhancement provides organizational officials the means to identify who reviewed and released the information. In the case of automated reviews, this control enhancement ensures that only approved review functions are employed.

Related Controls: AC-4, AC-16.

(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.

Supplemental Guidance: This control enhancement prevents the modification of information between review and transfer/release. The validation of bindings can be achieved, for example, using cryptographic checksums. Organizations determine validations are in response to user requests or generated automatically.

Related Controls: AC-4, AC-16.

(5) NON-REPUDIATION | DIGITAL SIGNATURES

[Withdrawn: Incorporated into SI-13].

References: FIPS Publications 140-2, 180-4, 186-4, 202; NIST Special Publication 800-177.

AU-11 AUDIT RECORD RETENTION

Control: Retain audit records for [*Assignment: organization-defined time-period consistent with records retention policy*] to provide support for after-the-fact investigations of security and privacy incidents and to meet regulatory and organizational information retention requirements.

Supplemental Guidance: Organizations retain audit records until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoenas, and law enforcement actions. Organizations develop standard categories of audit records relative to such types of actions and standard response processes for each type of action. The National Archives and Records Administration (NARA) General Records Schedules provide federal policy on record retention.

Related Controls: AU-2, AU-4, AU-5, AU-6, AU-9, AU-14, MP-6, RA-5, SI-12.

Control Enhancements:

(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.

Supplemental Guidance: This control enhancement helps to ensure that, from a technological perspective, audit records requiring long-term storage (on the order of years) can be accessed and read when needed. Measures employed by organizations to help facilitate the retrieval of audit records include, for example, converting records to newer formats, retaining equipment capable of reading the records, and retaining necessary documentation to help organizational personnel understand how to interpret the records.

Related Controls: None.

References: None.

AU-12 AUDIT GENERATION

Control:

a. Provide audit record generation capability for the auditable ~~events defined~~event types in AU-2 a. at [*Assignment: organization-defined system components*];

b. Allow [*Assignment: organization-defined personnel or roles*] to select which auditable ~~events~~event types are to be audited by specific components of the system; and

c. Generate audit records for the ~~events~~event types defined in AU-2 d. with the content in AU-3.

Supplemental Guidance: Audit records can be generated from many different system components. The list of audited ~~events~~event types is the set of ~~events~~event types for which audits are to be generated. These ~~events~~event types are ~~typically~~ a subset of all ~~events~~event types for which the system can generate audit records.

Related Controls: 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 SC-18, SI-3, SI-4, SI-7, SI-10.

Control Enhancements:

(1) AUDIT GENERATION | SYSTEM-WIDE AND TIME-CORRELATED AUDIT TRAIL

Compile audit records from [*Assignment: organization-defined system components*] into a system-wide (logical or physical) audit trail that is time-correlated to within [*Assignment: organization-defined level of tolerance for the relationship between time stamps of individual records in the audit trail*].

Supplemental Guidance: Audit trails are time-correlated if the time stamps in the individual audit records can be reliably related to the time stamps in other audit records to achieve a time ordering of the records within organizational tolerances.

Related Controls: AU-8.

(2) AUDIT GENERATION | STANDARDIZED FORMATS

Produce a system-wide (logical or physical) audit trail composed of audit records in a standardized format.

Supplemental Guidance: Audit information that is normalized to common standards promotes interoperability and exchange of such information between dissimilar devices and systems. This facilitates production of event information that can be more readily analyzed and correlated. Standard formats for audit records include, for example, system log records and audit records compliant with Common Event Expressions (CEE). If logging mechanisms within systems do not conform to standardized formats, systems may convert individual audit records into standardized formats when compiling system-wide audit trails.

Related Controls: None.

(3) AUDIT GENERATION | CHANGES BY AUTHORIZED INDIVIDUALS

Provide and implement the capability for [*Assignment: organization-defined individuals or roles*] to change the auditing to be performed on [*Assignment: organization-defined system components*] based on [*Assignment: organization-defined selectable event criteria*] within [*Assignment: organization-defined time thresholds*].

Supplemental Guidance: This control enhancement enables organizations to extend or limit auditing as necessary to meet organizational requirements. Auditing that is limited to conserve system resources may be extended to address certain threat situations. In addition, auditing may be limited to a specific set of event types to facilitate audit reduction, analysis, and reporting. Organizations can establish time thresholds in which audit actions are changed, for example, near real-time, within minutes, or within hours.

Related Controls: AC-3.

(4) AUDIT 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.

Supplemental Guidance: Query parameters are explicit criteria that a user or automated system submits to a system to retrieve data. Auditing of query parameters within systems for datasets that contain personally identifiable information augments an organization's ability to track and understand the access, usage, or sharing of personally identifiable information by authorized personnel.

Related Controls: None.

References: None.

AU-13 MONITORING FOR INFORMATION DISCLOSURE

Control: Monitor [*Assignment: organization-defined open source information and/or information sites*] [*Assignment: organization-defined frequency*] for evidence of unauthorized disclosure of organizational information.

Supplemental Guidance: Open source information includes, for example, social networking sites.

Related Controls: AC-22, PE-3, PM-12, RA-5, SC-7.

Control Enhancements:

(1) MONITORING FOR INFORMATION DISCLOSURE | USE OF AUTOMATED TOOLS

Employ automated mechanisms to determine if organizational information has been disclosed in an unauthorized manner.

Supplemental Guidance: Automated mechanisms can include, for example, automated scripts to monitor new posts on selected websites, and commercial services providing notifications and alerts to organizations.

Related Controls: None.

(2) MONITORING FOR INFORMATION DISCLOSURE | REVIEW OF MONITORED SITES

Review the open source information sites being monitored [*Assignment: organization-defined frequency*].

Supplemental Guidance: None.

Related Controls: None.

References: None.

AU-14 SESSION AUDIT

Control: Provide and implement the capability for authorized users to select a user session to capture/record or view/hear.

Supplemental Guidance: Session audits include, for example, monitoring keystrokes, tracking websites visited, and recording information and/or file transfers. Session auditing activities are developed, integrated, and used in consultation with legal counsel in accordance with applicable laws, Executive Orders, directives, policies, regulations, standard, and guidelines.

Related Controls: AC-3, AU-2, AU-3, AU-4, AU-5, AU-8, AU-9, AU-11, AU-12.

Control Enhancements:

(1) SESSION AUDIT | SYSTEM START-UP

Initiate session audits automatically at system start-up.

Supplemental Guidance: None.

Related Controls: None.

(2) SESSION AUDIT | CAPTURE AND RECORD ~~*AND LOG*~~ CONTENT

Provide and implement the capability for authorized users to capture, record, and log content related to a user session.

Supplemental Guidance: None.

Related Controls: None.

(3) SESSION AUDIT | REMOTE VIEWING AND LISTENING

Provide and implement the capability for authorized users to remotely view and hear content related to an established user session in real time.

Supplemental Guidance: None.

Related Controls: AC-17.

References: None.

AU-15 ALTERNATE AUDIT CAPABILITY

Control: Provide an alternate audit capability in the event of a failure in primary audit capability that ~~provides~~implements [*Assignment: organization-defined alternate audit functionality*].

Supplemental Guidance: Since an alternate audit capability may be a short-term protection employed until the failure in the primary auditing capability is corrected, organizations may determine that the alternate audit capability need only provide a subset of the primary audit functionality that is impacted by the failure.

Related Controls: AU-5, AU-9.

Control Enhancements: None.

References: None.

AU-16 CROSS-ORGANIZATIONAL AUDITING

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

Supplemental Guidance: When organizations use systems and/or services of external organizations, the auditing capability necessitates a coordinated approach across organizations. For example,

maintaining the identity of individuals that requested ~~particular~~specific services across organizational boundaries may often be very difficult, and doing so may prove to have significant performance and privacy ramifications. Therefore, it is often the case that cross-organizational auditing ~~(e.g., the type of auditing capability provided by service-oriented architectures)~~ simply captures the identity of individuals issuing requests at the initial system, and subsequent systems record that the requests emanated from authorized individuals.

Related Controls: AU-6, AU-7.

Control Enhancements:

(1) CROSS-ORGANIZATIONAL AUDITING | IDENTITY PRESERVATION

Require that the identity of individuals is preserved in cross-organizational audit trails.

Supplemental Guidance: This control enhancement applies when there is a need to be able to trace actions that are performed across organizational boundaries to a specific individual.

Related Controls: IA-2, IA-4, IA-5, IA-8.

(2) CROSS-ORGANIZATIONAL AUDITING | SHARING OF AUDIT INFORMATION

Provide cross-organizational audit information to [*Assignment: organization-defined organizations*] based on [*Assignment: organization-defined cross-organizational sharing agreements*].

Supplemental Guidance: Because of the distributed nature of the audit information, cross-organization sharing of audit information may be essential for effective analysis of the auditing being performed. For example, the audit records of one organization may not provide sufficient information to determine the appropriate or inappropriate use of organizational information resources by individuals in other organizations. In some instances, only the home organizations of individuals have the appropriate knowledge to make such determinations, thus requiring the sharing of audit information among organizations.

Related Controls: IR-4, SI-4.

References: None.

3.4 ASSESSMENT, AUTHORIZATION, AND MONITORING

Quick link to Assessment, Authorization, and Monitoring summary table

CA-1 ASSESSMENT, AUTHORIZATION~~SECURITY ASSESSMENT AND AUTHORIZATION~~, AND MONITORING POLICY AND PROCEDURES

Control:

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

1. A security and privacy 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

~~1.~~2. Procedures to facilitate the implementation of the security and privacy assessment, authorization, and monitoring policy and the associated security and privacy assessment, authorization, and monitoring controls;

b. Designate an [*Assignment: organization-defined senior management official*] to manage the security and privacy assessment, authorization, and monitoring policy and procedures;

~~b.~~c. Review and update the current security and privacy assessment, authorization, and monitoring:

1. Policy [*Assignment: organization-defined frequency*]; and

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

d. Ensure that the security and privacy assessment, authorization, and monitoring procedures implement the security and privacy assessment, authorization, and monitoring policy and controls; and

e. Develop, document, and implement remediation actions for violations of security and privacy assessment, authorization, and monitoring policy.

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of ~~selected security~~ the controls and control enhancements in the CA family. The risk management strategy is an important factor in establishing policy and procedures ~~reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards,~~. Comprehensive policy and ~~guidance.~~procedures help provide security and privacy assurance. Security and privacy program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general ~~information~~ security and privacy policy ~~for organizations or conversely,~~or can be represented by multiple policies reflecting the complex nature of ~~certain~~ organizations. The procedures can be established for security ~~program in general~~and privacy programs and for ~~particular information~~ systems, if needed. Procedures describe how policies or controls are implemented and can be directed at the personnel 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. It is important to recognize that restating controls does not constitute an organizational ~~risk management strategy is a key factor in establishing~~ policy ~~and procedures~~or procedure.

Related Controls: PM-9, PS-8, SI-12.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-30, 800-39, 800-50, 800-100, 800-122; NIST Interagency Report 8062.

CA-2 ~~SECURITY~~ ASSESSMENTS

Control:

a. Develop a security and privacy assessment plan that describes the scope of the assessment including:

   1. Security and privacy controls and control enhancements under assessment;

   2. Assessment procedures to be used to determine ~~security~~ control effectiveness; and

   3. Assessment environment, assessment team, and assessment roles and responsibilities;

b. Ensure the assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment;

~~b.~~c. Assess the security and privacy 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;

~~c.~~d. Produce a security and privacy assessment report that document the results of the assessment; and

~~d.~~e. Provide the results of the security and privacy control assessment to [*Assignment: organization-defined individuals or roles*].

Supplemental Guidance: Organizations assess security and privacy controls in organizational systems and the environments in which those systems operate as part of initial and ongoing authorizations; FISMA annual assessments; continuous monitoring; and system development life cycle activities. Assessments ensure that organizations meet information security ~~is built into organizational information systems;~~and privacy requirements; identify weaknesses and deficiencies ~~early~~ in the development process; provide essential information needed to make risk-based decisions as part of authorization processes; and ensure compliance to vulnerability mitigation procedures. Organizations conduct assessments on the implemented controls from Chapter Three as documented in ~~System~~ security plans and ~~Information Security Program~~privacy plans. 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 entire life cycle. Assessment reports document assessment results in sufficient detail as deemed necessary by organizations, to determine the accuracy and completeness of the reports and whether the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting ~~security requirements. The FISMA requirement for assessing security controls at least annually does not require additional assessment activities to those activities already in place in organizational security authorization processes. Security~~requirements. Assessment results are provided to the individuals or roles appropriate for the types of assessments being conducted. For example, assessments conducted in support of authorization decisions are provided to authorizing officials, senior agency officials for privacy, and/or authorizing official designated representatives.

To satisfy annual assessment requirements, organizations can use assessment results from the following sources: initial or ongoing system authorizations; continuous monitoring; or system development life cycle activities. Organizations ensure that assessment results are current, relevant to the determination of control effectiveness, and obtained with the appropriate level of assessor independence. Existing control assessment results can be reused to the extent that the results are still valid and can also be supplemented with additional assessments as needed. After the initial authorizations ~~and in accordance with OMB policy~~, organizations assess controls during continuous monitoring. Organizations also establish the frequency for ongoing assessments in accordance with organizational continuous monitoring strategies. ~~Information Assurance~~

~~Vulnerability Alerts provide useful examples of vulnerability mitigation procedures.~~ External audits including, for example, audits by external entities such as regulatory agencies, are outside the scope of this control.

Related Controls: AC-20, CA-5, CA-6, CA-7, PM-9, RA-5, SA-11, SA-12, SC-38, SI-3, SI-12.

Control Enhancements:

(1) ~~*SECURITY*~~ ASSESSMENTS | INDEPENDENT ASSESSORS

Employ independent assessors or assessment teams to conduct security and privacy control assessments.

Supplemental Guidance: Independent assessors or assessment teams are individuals or groups conducting impartial assessments of systems. Impartiality implies that assessors are free from any perceived or actual conflicts of interest regarding development, operation, sustainment, or management of the systems under assessment or the determination of control effectiveness. To achieve impartiality, assessors should 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 can be contracted to public or private sector entities outside of organizations. Authorizing officials determine the required level of independence based on the security categories of 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. This includes determining whether contracted assessment services have sufficient independence, for example, when system owners are not directly involved in contracting processes or cannot ~~unduly~~ influence the impartiality of assessors conducting assessments. ~~In special situations, for example,~~ When organizations that own the systems are small or organizational structures require that assessments are conducted by individuals that are in the developmental, operational, or management chain of system owners, independence in assessment processes can be achieved by ensuring that assessment results are carefully reviewed and analyzed by independent teams of experts to validate the completeness, accuracy, integrity, and reliability of the results. Organizations recognize that assessments performed for purposes other than direct support to authorization decisions are, when performed by assessors with sufficient independence, more likely to be useable for such decisions, thereby reducing the need to repeat assessments.

Related Controls: None.

(2) ASSESSMENTS | SPECIALIZED ASSESSMENTS

Include as part of security and privacy control assessments, [*Assignment: organization-defined frequency*], [*Selection: announced; unannounced*], [*Selection (one or more): in-depth monitoring; vulnerability scanning; malicious user testing; insider threat assessment; performance~~/~~ and load testing;* [*Assignment: organization-defined other forms of ~~security~~ assessment*]].

Supplemental Guidance: Organizations can ~~employ information system monitoring,~~ conduct specialized assessments including, for example, verification, validation, insider threat assessments, malicious user testing, system monitoring, and other forms of testing ~~(e.g., verification and validation) to~~. Such assessments can improve readiness by exercising organizational capabilities and indicating current performance levels as a means of focusing actions to improve security and privacy. Organizations conduct ~~assessment activities~~these types of specialized assessments in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidelines. Authorizing officials approve the assessment methods in coordination with the organizational risk executive function. Organizations can incorporate vulnerabilities uncovered during assessments into vulnerability remediation processes.

Related Controls: PE-3, SI-2.

(3) ASSESSMENTS | EXTERNAL ORGANIZATIONS

Accept the results of ~~an assessment~~security and privacy control assessments of [*Assignment: organization-defined ~~information~~ system*] performed by [*Assignment: organization-defined external organization*] when the assessment meets [*Assignment: organization-defined requirements*].

Supplemental Guidance: Organizations may ~~often~~ rely on security and privacy control assessments of ~~specific information~~ organizational systems by other (external) organizations. Using such assessments and reusing existing assessment evidence can significantly decrease the time and resources required for assessments by limiting the amount of independent assessment activities that organizations need to perform. The factors that organizations consider in determining whether to accept assessment results from external organizations can vary. ~~Determinations for accepting assessment results can be based on~~Such factors include, for example, past assessment experiences ~~one~~the organization has had with ~~another~~the organization~~,~~ conducting the assessment; the reputation that ~~organizations have~~the assessing organization has with regard to assessments~~,~~; the level of detail of supporting assessment ~~documentation~~evidence provided~~, or~~; and the mandates imposed ~~upon organizations~~ by ~~federal legislation~~applicable laws, Executive Orders, directives, policies, ~~or directives~~regulations, standards, and guidelines.

Related Controls: None.

References: FIPS Publication 199; NIST Special Publications 800-37, 800-39, 800-53A, 800-115, 800-122, 800-137; NIST Interagency Report 8062.

CA-3 SYSTEM INTERCONNECTIONS

Control:

a. Authorize connections from the system to other systems using Interconnection Security Agreements;

b. Document, for each interconnection, the interface characteristics, security and privacy requirements, and the nature of the information communicated; and

c. Review and update Interconnection Security Agreements [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control applies to dedicated connections between two or more separate systems ~~(i.e., system interconnections)~~ and does not apply to transitory, user-controlled connections such as email and website browsing. Organizations consider the risks that may be introduced when systems are connected to other systems with different security and privacy requirements and ~~security~~ controls, ~~both~~including systems within ~~organizations~~the same organization and systems external to the organization. Authorizing officials determine the risk associated with system connections and the appropriate controls employed. If interconnecting systems have the same authorizing official, organizations do not need to develop Interconnection Security Agreements. Instead, those organizations can describe the interface characteristics between the interconnecting systems in their respective security and privacy plans. If interconnecting systems have different authorizing officials within the same organization, the organizations can develop Interconnection Security Agreements or they can describe the interface characteristics between the systems in the security and privacy plans for the respective systems. Organizations may also incorporate Interconnection Security Agreement information into formal contracts, especially for interconnections established between federal agencies and nonfederal ~~(i.e., private sector)~~ organizations. Risk considerations also include systems sharing the same networks. ~~For certain technologies (e.g., space, unmanned aerial vehicles,~~As part of the risk assessment of connecting to external systems, organizations consider the number and ~~medical devices), there may be specialized~~types of transitive connections ~~in place during preoperational testing.~~that exist when establishing such connections ~~may require Interconnection Security Agreements and be subject to additional security controls.~~.

Related Controls: AC-20, AU-16, IA-3, PL-2, RA-3, SA-9, SC-7, SI-12.

Control Enhancements:

(1) SYSTEM INTERCONNECTIONS | UNCLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS

Prohibit the direct connection of an [*Assignment: organization-defined unclassified, national security system*] to an external network without the use of [*Assignment: organization-defined boundary protection device*].

Supplemental Guidance: Organizations typically do not have control over external networks including the Internet. Approved boundary protection devices including, for example, routers and firewalls. mediate communications and information flows between unclassified national security systems and external networks. ~~This control enhancement is required for organizations processing, storing, or transmitting Controlled Unclassified Information (CUI).~~

Related Controls: None.

(2) SYSTEM INTERCONNECTIONS | 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*].

Supplemental Guidance: Organizations typically do not have control over external networks including the Internet. Approved boundary protection devices including, for example, routers and firewalls, mediate communications and information flows between classified national security systems and external networks. In addition, approved boundary protection devices (typically managed interface/cross-domain systems) provide information flow enforcement from systems to external networks.

Related Controls: None.

(3) SYSTEM INTERCONNECTIONS | UNCLASSIFIED NON-NATIONAL SECURITY SYSTEM CONNECTIONS

Prohibit the direct connection of an [*Assignment: organization-defined unclassified, non-national security system*] to an external network without the use of [*Assignment; organization-defined boundary protection device*].

Supplemental Guidance: Organizations typically do not have control over external networks including the Internet. Approved boundary protection devices including, for example, routers and firewalls mediate communications and information flows between unclassified non-national security systems and external networks. ~~This control enhancement is required for organizations processing, storing, or transmitting Controlled Unclassified Information (CUI).~~

Related Controls: None.

(4) SYSTEM INTERCONNECTIONS | CONNECTIONS TO PUBLIC NETWORKS

Prohibit the direct connection of an [*Assignment: organization-defined system*] to a public network.

Supplemental Guidance: A public network is any network accessible to the general public including, for example, the Internet and organizational extranets with public access.

Related Controls: None.

(5) SYSTEM INTERCONNECTIONS | RESTRICTIONS ON EXTERNAL SYSTEM CONNECTIONS

~~**The organization employs [*Selection: allow-all, deny-by-exception;*]**~~**Employ a deny-all, permit-by-exception~~**]** **policy for allowing [*Assignment: organization-defined systems*] to connect to external systems.**

Supplemental Guidance: Organizations can constrain system connectivity to external domains ~~(e.g., websites)~~ by employing ~~one of two policies with regard to such connectivity: (i) allow-all, deny-by-exception, also known as *blacklisting* (the weaker of the two policies); or (ii) deny-all, allow-by-exception, also~~a deny-all, permit-by-exception policy known as *whitelisting* ~~(the stronger of the two policies). For either policy,~~. Organizations determine what exceptions, if any, are acceptable. This control~~: CM~~ enhancement is applied to a system that is connected to another system. Alternatively, control enhancement SC-7(5) applies to any type of network communications.

Related Controls: SC-7.

(6) SYSTEM INTERCONNECTIONS | SECONDARY AND TERTIARY CONNECTIONS

(a) Identify secondary and tertiary connections to the interconnected systems; and

(b) Take measures to ensure that connections are severed when security and privacy controls on identified secondary and tertiary systems cannot be verified or validated.

Supplemental Guidance: For certain critical systems and applications including, for example, high-value assets, it may be necessary to identify second and third level connections to the interconnected systems. The transparency of the protection measures in place in secondary and tertiary systems connected directly or indirectly to organizational systems is essential in understanding the actual security and privacy risks resulting from those interconnections. Organizational systems can inherit risk from secondary and tertiary systems through those connections and make the organizational systems more susceptible to threats, hazards, and adverse consequences.

Related Controls: None.

References: FIPS Publication 199; NIST Special Publication 800-47.

CA-4 SECURITY CERTIFICATION

[Withdrawn: Incorporated into CA-2].

CA-5 PLAN OF ACTION AND MILESTONES

Control:

a. Develop a plan of action and milestones for the system to document the planned remedial 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, impact analyses, and continuous monitoring activities.

Supplemental Guidance: Plans of action and milestones are required documents in authorization packages and are subject to federal reporting requirements established by OMB.

Related Controls: CA-2, CA-7, PM-4, PM-9, RA-7, SI-2, SI-12.

Control Enhancements:

(1) PLAN OF ACTION AND MILESTONES | AUTOMATION SUPPORT FOR ACCURACY AND CURRENCY

Employ automated mechanisms to ensure that the plan of action and milestones for the system is accurate, up to date, and readily available.

Supplemental Guidance: None.

Related Controls: None.

References: NIST Special Publication 800-37.

CA-6 ~~SECURITY~~ AUTHORIZATION

Control:

a. Assign a senior-level executive or manager as the authorizing official for the system and for any common controls inherited by the system;

b. Ensure that the authorizing official, before commencing operations:

1. ~~Updates~~Authorizes the ~~security authorization~~system for processing; and

2. Authorizes the common controls inherited by the system; and

c. Update the authorizations [*Assignment: organization-defined frequency*].

Supplemental Guidance: ~~Security~~ Authorizations are official management decisions~~, conveyed through authorization decision documents,~~ by senior ~~organizational~~ officials ~~or executives (i.e., authorizing officials)~~ to authorize operation of systems (including the controls inherited by those systems) and to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of agreed-upon security and privacy controls. Authorizing officials provide budgetary oversight for organizational systems or assume

responsibility for the mission and business operations supported by those systems. The ~~security~~ authorization process is ~~an inherently~~a federal responsibility and therefore, authorizing officials must be federal employees. ~~Through the security authorization process,~~ Authorizing officials are responsible and accountable for security and privacy risks associated with the operation and use of organizational systems. ~~Accordingly, authorizing~~Nonfederal organizations may have similar processes to authorize their systems and senior officials ~~are in positions with levels of authority commensurate with understanding and accepting such information security-related risks. OMB policy requires~~ that assume the authorization role and associated responsibilities. Organizations conduct ongoing authorizations of systems by implementing continuous monitoring programs. Robust continuous monitoring programs ~~can satisfy three-year reauthorization requirements, so~~reduce the need for separate reauthorization processes ~~are not necessary~~. Through the employment of comprehensive continuous monitoring processes, critical information contained in authorization packages including the security and privacy plans, security and privacy assessment reports, and plans of action and milestones, is updated on an ongoing basis. This provides authorizing officials, system owners, and common control providers with an up-to-date status of the security and privacy state of their systems, controls, and environments of operation. To reduce the ~~administrative~~ cost of reauthorization, authorizing officials use the results of continuous monitoring processes to the maximum extent possible as the basis for rendering reauthorization decisions.

Related Controls: CA-2, CA-7, PM-9, PM-10, SA-10, SI-12.

Control Enhancements:

(1) AUTHORIZATION | JOINT AUTHORIZATION — SAME ORGANIZATION

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

Supplemental Guidance: Assigning multiple authorizing officials from the same organization to serve as co-authorizing officials for the system, increases the level of independence in the risk-based decision making process for security and privacy. It also implements the concepts of separation of duties and dual authorization as applied to the system authorization process. This enhancement is most relevant for interconnected systems, shared systems, and systems with one or more information owners.

Related Controls: AC-6.

(2) AUTHORIZATION | JOINT AUTHORIZATION — DIFFERENT ORGANIZATIONS

Employ a joint authorization process for the system that includes multiple authorizing officials with at least one authorizing official from an organization external to the organization conducting the authorization.

Supplemental Guidance: Assigning multiple authorizing officials, at least one of which comes from an external organization, to serve as co-authorizing officials for the system, increases the level of independence in the risk-based decision making process for security and privacy. It also implements the concepts of separation of duties and dual authorization and as applied to the system authorization process. Employing authorizing officials from external organizations to supplement the authorization official from the organization owning or hosting the system may be necessary when those organizations have a vested interest or equities in the outcome of the authorization decision. This situation may occur with interconnected systems, shared systems, and systems with one or more information owners. Accordingly, the authorizing officials from the external organizations may be considered key stakeholders of the system undergoing authorization.

Related Controls: AC-6.

References: NIST Special Publications 800-37, 800-137; NIST Supplemental Guidance on Ongoing Authorization.

CA-7 CONTINUOUS MONITORING

Control: Develop a security and privacy continuous monitoring strategy and implement security and privacy continuous monitoring programs that include:

a. Establishing the following security and privacy metrics to be monitored: [*Assignment: organization-defined metrics*];

b. Establishing [*Assignment: organization-defined frequencies*] for monitoring and [*Assignment: organization-defined frequencies*] for ~~assessments supporting such monitoring~~ongoing assessment of security and privacy control effectiveness;

c. Ongoing security and privacy control assessments in accordance with the organizational continuous monitoring strategy;

d. Ongoing security and privacy status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy;

e. Correlation and analysis of security- and privacy-related information generated by security and privacy control assessments and monitoring;

f. Response actions to address results of the analysis of security- and privacy-related information; and

g. Reporting the security and privacy status of the organization and organizational systems to [*Assignment: organization-defined personnel or roles*] [*Assignment: organization-defined frequency*].

Supplemental Guidance: Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security and privacy to support organizational risk management decisions. The terms continuous and ongoing imply that organizations assess~~/analyze~~ security and privacy controls and associated risks at a frequency sufficient to support ~~organizational~~ risk-based decisions. The results of continuous monitoring ~~programs~~ generate ~~appropriate~~ risk response actions by organizations. When monitoring the effectiveness of 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 also allow organizations to maintain the ~~security~~ authorizations of systems and common controls over time in highly dynamic environments of operation with changing mission and business needs, threats, vulnerabilities, and technologies. Having access to security- and privacy-related information on a continuing basis through reports and dashboards gives organizational officials the capability to make more 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.

Related Controls: AC-2, AC-6, AU-6, CA-2, CA-5, CA-6, CM-3, CM-4, CM-6, CM-11, IA-5, PE-6, PL-2, PM-4, PM-6, PM-9, PM-10, PM-12, PM-14, PM-32, RA-3, RA-5, RA-7, SA-11, SC-5, SC-38, SI-3, SI-4, SI-12.

Control Enhancements:

(1) CONTINUOUS MONITORING | INDEPENDENT ASSESSMENT

Employ independent assessors or assessment teams ~~with [*Assignment: organization-defined level of independence*]~~ to monitor the security and privacy controls in the system on an ongoing basis.

Supplemental Guidance: Organizations can maximize the value of control assessments during the continuous monitoring process by requiring that assessments be conducted by assessors with appropriate levels of independence. The level of assessor independence required is based on organizational continuous monitoring strategies. Assessor independence provides a degree of impartiality to the monitoring process. To achieve such impartiality, assessors should 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.

Related Controls: None.

(2) CONTINUOUS MONITORING | TYPES OF ASSESSMENTS

[Withdrawn: Incorporated into CA-2].

(3) CONTINUOUS MONITORING | TREND ANALYSES

Employ trend analyses to determine if security and privacy 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.

Supplemental Guidance: Trend analyses can include, for example, examining recent threat information regarding the types of threat events that have occurred within the organization or the federal government, success rates of certain types of attacks, emerging vulnerabilities in ~~information~~specific technologies, evolving social engineering techniques, results from multiple control assessments, the effectiveness of configuration settings, and findings from Inspectors General or auditors.

Related Controls: None.

(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.

Supplemental Guidance: Effectiveness monitoring determines the ongoing effectiveness of implemented risk response measures. Compliance monitoring verifies that the 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.

Related Controls: None.

References: NIST Special Publications 800-37, 800-39, 800-53A, 800-115, 800-122, 800-137; NIST Interagency Reports 8011, 8062.

CA-8 PENETRATION TESTING

Control: Conduct penetration testing [*Assignment: organization-defined frequency*] on [*Assignment: organization-defined systems or system components*].

Supplemental Guidance: 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 most effectively conducted by penetration testing agents and teams with demonstrable skills and experience that, depending on the scope of the penetration testing, include technical expertise in network, operating system, and/or application level security. Penetration testing can be used to either validate vulnerabilities or determine the degree of penetration resistance of systems to adversaries within specified constraints. Such constraints include, for example, time, resources, and skills. Penetration testing attempts to duplicate the actions of adversaries in carrying out ~~hostile cyber~~ attacks against organizations and provides a more in-depth analysis of security- and privacy-related weaknesses or deficiencies. Organizations can use the results of vulnerability analyses to support penetration testing activities. Penetration testing can be conducted 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, for example, pretest analysis based on full knowledge of the target system; pretest identification of potential vulnerabilities based on pretest analysis; and testing designed to determine exploitability of identified vulnerabilities. All parties agree to the rules of engagement before commencement of 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 carrying out attacks. Risk assessments guide the decisions on the level of independence required for personnel conducting penetration testing.

Related Controls: SA-11, SA-12.

Control Enhancements:

(1) PENETRATION TESTING | INDEPENDENT PENETRATION AGENT OR TEAM

Employ an independent penetration agent or penetration team to perform penetration testing on the system or system components.

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

Related Controls: CA-2.

(2) PENETRATION TESTING | RED TEAM EXERCISES

Employ [*Assignment: organization-defined red team exercises*] to simulate attempts by adversaries to compromise organizational systems in accordance with [~~*Assignment: organization-defined*~~applicable] rules of engagement.

Supplemental Guidance: Red team exercises extend the objectives of penetration testing by examining the security and privacy posture of organizations and their ability to implement effective cyber defenses. Red team exercises reflect simulated attempts by adversaries to compromise organizational missions and business functions and provide a comprehensive assessment of the security and privacy state of systems and organizations. Simulated attempts by adversaries to compromise missions and business functions and the systems that support those missions and functions may include technology-~~focused attacks (e.g.,~~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 effectively 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. Red team exercises can be used to improve security and privacy awareness and training and to assess ~~levels of security~~ control effectiveness.

Related Controls: None.

(3) PENETRATION TESTING | FACILITY PENETRATION TESTING

Employ a penetration testing process that includes [*Assignment: organization-defined frequency*] [*Selection: announced; unannounced*] attempts to bypass or circumvent controls associated with physical access points to the facility.

Supplemental Guidance: None.

Related Controls: CA-2, PE-3.

References: None.

CA-9 INTERNAL SYSTEM CONNECTIONS

Control:

a. Authorize internal connections of [*Assignment: organization-defined system components or classes of components*] to the system; and

b. Document, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated.

Supplemental Guidance: This control applies to connections between organizational systems and separate constituent system components. These intra-system connections, include, for example, system connections with mobile devices, notebook computers, desktop computers, workstations, printers, copiers, facsimile machines, scanners, sensors, and servers. Instead of authorizing each individual internal system connection, organizations can authorize internal connections for a class of system components with common characteristics and/or configurations. This can include, for example, all digital printers, scanners, and copiers with a specified processing, transmission, and storage capability or all smart phones with a specific baseline configuration.

Related Controls: AC-3, AC-4, AC-18, AC-19, CM-2, IA-3, SC-7, SI-12.

Control Enhancements:

(1) INTERNAL SYSTEM CONNECTIONS | COMPLIANCE CHECKS

Perform security and privacy compliance checks on constituent system components prior to the establishment of the internal connection.

Supplemental Guidance: Compliance checks may include, for example, verification of the relevant baseline configuration.

Related Controls: CM-6.

References: NIST Special Publication 800-124; NIST Interagency Report 8023.

3.5 CONFIGURATION MANAGEMENT

Quick link to Configuration Management summary table

CM-1 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES

Control:

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

1. A 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 senior management official*] to manage configuration management policy and procedures;

~~b.~~c. Review and update the current configuration management:

1. Policy [*Assignment: organization-defined frequency*]; and

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

d. Ensure that the configuration management procedures implement the configuration management policy and controls; and

e. Develop, document, and implement remediation actions for violations of the configuration management policy.

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of ~~selected security~~ the controls and control enhancements in the CM family. The risk management strategy is an important factor in establishing policy and procedures ~~reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards,~~. Comprehensive policy and ~~guidance.~~procedures help provide security and privacy assurance. Security and privacy program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general ~~information~~ security and privacy policy ~~for organizations~~ or ~~conversely,~~ can be represented by multiple policies reflecting the complex nature of ~~certain~~ organizations. The procedures can be established for ~~the~~ security ~~program in general~~and privacy programs and for ~~particular information~~ systems, if needed. ~~The~~Procedures describe how policies or controls are implemented and can be directed at the personnel 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. It is important to recognize that restating controls does not constitute an organizational ~~risk management strategy is a key factor in establishing policy and procedures.~~ policy or procedure.

Related Controls: PM-9, PS-8, SI-12.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-30, 800-39, 800-100.

CM-2 BASELINE CONFIGURATION

Control:

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.

Supplemental Guidance: This control establishes baseline configurations for systems and system components including communications and connectivity-related aspects of systems. Baseline configurations are documented, formally reviewed and agreed-upon sets of specifications for systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, and/or changes to systems. Baseline configurations include information about system components ~~(e.g., standard software packages installed on workstations, notebook computers, servers, network components, or mobile devices; current version numbers and patch information on operating systems and applications; and configuration settings/parameters),~~ network topology, and the logical placement of those components within the system architecture. Maintaining baseline configurations requires creating new baselines as organizational systems change over time. Baseline configurations of systems reflect the current enterprise architecture.

Related Controls: AC-19, AU-6, CA-9, CM-1, CM-3, CM-5, CM-6, CM-8, CM-9, CP-9, CP-10, CP-12, PL-8, PM-5, SA-10, SC-18.

Control Enhancements:

~~(1)~~ BASELINE CONFIGURATION | REVIEWS AND UPDATES ~~**The organization reviews and updates the baseline configuration of the information system:**~~

~~(2)~~(1) ~~[*Assignment: organization-defined frequency*];When required due to [*Assignment organization-defined circumstances*]; and~~

~~**a. As an integral part of information system component installations and upgrades.**~~

~~Supplemental Guidance: Related control: CM-5.~~

[Withdrawn: Incorporated into CM-2].

~~(3)~~(2) BASELINE CONFIGURATION | AUTOMATION SUPPORT FOR ACCURACY AND CURRENCY

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

Supplemental Guidance: Automated mechanisms that help organizations maintain consistent baseline configurations for systems include, for example, hardware and software inventory tools, configuration management tools, and network management tools. Such tools can be deployed and/or allocated as common controls, at the system level, or at the operating system or component level including, for example, on workstations, servers, notebook computers, network components, or mobile devices. Tools can be used, for example, to track version numbers on operating systems, applications, types of software installed, and current patch levels. This control enhancement can be satisfied by the implementation of CM-8(2) for organizations that choose to combine system component inventory and baseline configuration activities.

Related Controls: CM-7, IA-3, RA-5.

~~(4)~~(3) BASELINE CONFIGURATION | RETENTION OF PREVIOUS CONFIGURATIONS

Retain [*Assignment: organization-defined previous versions of baseline configurations of the system*] to support rollback.

Supplemental Guidance: Retaining previous versions of baseline configurations to support rollback may include, for example, hardware, software, firmware, configuration files, and configuration records.

Related Controls: None.

~~(5)~~(4) BASELINE CONFIGURATION | UNAUTHORIZED SOFTWARE

[Withdrawn: Incorporated into CM-7(4)].

~~(6)~~(5) BASELINE CONFIGURATION | AUTHORIZED SOFTWARE

[Withdrawn: Incorporated into CM-7(5)].

~~(7)~~(6) BASELINE CONFIGURATION | DEVELOPMENT AND TEST ENVIRONMENTS

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

Supplemental Guidance: Establishing separate baseline configurations for development, testing, and operational environments helps protect systems from unplanned/unexpected events related to development and testing activities. Separate baseline configurations allow organizations to apply the configuration management that is most appropriate for each type of configuration. For example, management of operational configurations typically emphasizes the need for stability, while management of development/test configurations requires greater flexibility. Configurations in the test environment mirror the configurations in the operational environment to the extent practicable so that the results of the testing are representative of the proposed changes to the operational systems. This control enhancement requires separate configurations but not necessarily separate physical environments.

Related Controls: CM-4, SC-3, SC-7.

~~(8)~~(7) BASELINE CONFIGURATION | CONFIGURE SYSTEMS AND COMPONENTS~~, OR DEVICES~~ 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 [*Assignment: organization-defined security safeguards*] to the components when the individuals return from travel.

Supplemental Guidance: When it is known that systems or system components~~, or devices (e.g., notebook computers, mobile devices)~~ will be in high-risk areas, additional ~~security~~ controls may be implemented to counter the ~~greater~~increased threat in such areas ~~coupled with the lack of physical security relative to organizational-controlled areas.~~. For example, ~~organizational policies and procedures~~organizations can take specific actions for notebook computers used by individuals departing on and returning from travel. These actions can include, for example, determining which locations are of concern, defining required configurations for the devices, ensuring that the devices are configured as intended before travel is initiated, and applying specific safeguards to the ~~device~~component after travel is completed. Specially configured notebook computers include, for example, computers with sanitized hard drives, limited applications, and ~~additional hardening (e.g.,~~ more stringent configuration settings. Specified safeguards applied to mobile devices upon return from travel include, for example, examining the device for signs of physical tampering; and purging and reimaging the hard disk drive. Protecting information residing on mobile devices is covered in the media protection family.

Related Controls: None.

References: NIST Special Publications 800-124, 800-128.

CM-3 CONFIGURATION CHANGE CONTROL

Control:

a. Determine 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 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. ~~Audits~~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*]; [*Assignment: organization-defined configuration change conditions*]].

Supplemental Guidance: Configuration change controls for organizational systems involve the systematic proposal, justification, implementation, testing, review, and disposition of changes to the systems, including system upgrades and modifications. Configuration change control includes changes to baseline configurations for components and configuration items of systems; changes to configuration settings for ~~information technology~~component products ~~(e.g., operating systems, applications, firewalls, routers, and mobile devices),;~~ unscheduled or unauthorized changes; and changes to remediate vulnerabilities. Configuration change control elements can include such entities as committees or boards. Typical processes for managing configuration changes to ~~information~~ systems include, for example, Configuration Control Boards or Change Advisory Boards that review and approve proposed changes to systems. For new development ~~information~~ systems or systems undergoing major upgrades, organizations consider including representatives from development organizations on the Configuration Control Boards or Change Advisory Boards. Auditing of changes includes activities before and after changes are made to organizational systems and the auditing activities required to implement such changes.

Related Controls: CA-7, CM-2, CM-4, CM-5, CM-6, CM-9, CM-11, IA-3, MA-2, PE-16, SA-10, SA-19, SC-28, SC-34, SC-37, SI-2, SI-3, SI-4, SI-7, SI-10.

Control Enhancements:

(1) CONFIGURATION CHANGE CONTROL | AUTOMATED DOCUMENTATION, NOTIFICATION, AND PROHIBITION OF CHANGES

Employ automated mechanisms to:

(a) Document proposed changes to the system;

(b) Notify [*Assignment: organized-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 by [*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.

Supplemental Guidance: None.

Related Controls: None.

(2) CONFIGURATION CHANGE CONTROL | TESTING, VALIDATION, AND DOCUMENTATION OF CHANGES

Test, validate, and document changes to the system before fully implementing the changes on the ~~operational~~ system.

Supplemental Guidance: 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. Individuals or groups conducting tests understand organizational 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 off-line, or replicated to the extent feasible, before testing can be conducted. If systems must be taken off-line 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~~(e.g., testing on replicated systems).~~

Related Controls: None.

(3) CONFIGURATION CHANGE CONTROL | AUTOMATED CHANGE IMPLEMENTATION

Employ automated mechanisms to implement changes to the current system baseline and deploy the updated baseline across the installed base.

Supplemental Guidance: None.

Related Controls: None.

(4) CONFIGURATION CHANGE CONTROL | SECURITY REPRESENTATIVE

Require an [*Assignment: organization-defined* information security representative] to be a member of the [*Assignment: organization-defined configuration change control element*].

Supplemental Guidance: Information security representatives can include, for example, Senior Agency Information Security Officers, system security officers, or system security managers. Representation by personnel with information security expertise is important because changes to system configurations can have unintended side effects, some of which may be security-relevant. Detecting such changes early in the process can help avoid unintended, negative consequences that could ultimately affect the security state of organizational systems. The configuration change control element in this control enhancement reflects the change control elements defined by organizations in CM-3.

Related Controls: None.

(5) CONFIGURATION CHANGE CONTROL | AUTOMATED SECURITY RESPONSE

Implement [*Assignment: organization-defined security responses*] automatically if baseline configurations are changed in an unauthorized manner.

Supplemental Guidance: Security responses include, for example, halting system processing, halting selected system functions, or issuing alerts or notifications to organizational personnel when there is an unauthorized modification of a configuration item.

Related Controls: None.

(6) CONFIGURATION CHANGE CONTROL | CRYPTOGRAPHY MANAGEMENT

Ensure that cryptographic mechanisms used to provide [*Assignment: organization-defined security safeguards*] are under configuration management.

Supplemental Guidance: Regardless of the cryptographic means employed ~~(e.g., public key, private key, shared secrets),~~ organizations ensure that there are processes and procedures in place to ~~effectively~~ manage those means. For example, if devices use certificates ~~as a basis~~ for identification and authentication, ~~there needs to be~~ a process ~~in place~~is implemented to address the expiration of those certificates.

Related Controls: SC-12.

References: NIST Special Publications 800-124, 800-128; NIST Interagency Report 8062.

CM-4 SECURITY AND PRIVACY IMPACT ANALYSES

Control: Analyze changes to the system to determine potential security and privacy impacts prior to change implementation.

Supplemental Guidance: Organizational personnel with security or privacy responsibilities ~~(e.g., Information System Administrators, Information System Security Officers, Information System Security Managers, and Information System Security Engineers)~~ conduct ~~security~~ impact analyses. Individuals conducting ~~security~~ impact analyses possess the necessary skills and technical expertise to analyze the changes to systems and the associated security or privacy ramifications. Security and privacy impact analyses include, for example, reviewing security and privacy plans, policies, and procedures to understand security and privacy control requirements; reviewing system design documentation to understand control implementation and how specific changes might affect the controls; and determining how potential changes to a system create new risks to the privacy of individuals and the ability of implemented controls to mitigate those risks. Impact analyses may also include assessments of risk to better understand the impact of the changes and to determine if additional security or privacy controls are required.

Related Controls: CA-7, CM-3, CM-8, CM-9, MA-2, RA-5, SA-5, SA-10, SI-2.

Control Enhancements:

(1) SECURITY AND PRIVACY IMPACT ANALYSES | SEPARATE TEST ENVIRONMENTS

Analyze changes to the system in a separate test environment before implementation in an operational environment, looking for security and privacy impacts due to flaws, weaknesses, incompatibility, or intentional malice.

Supplemental Guidance: Separate test environment in this context means an environment that is physically or logically isolated and distinct from the operational environment. The separation is sufficient to ensure that activities in the test environment do not impact activities in the operational environment, and information in the operational environment is not inadvertently transmitted to the test environment. Separate environments can be achieved by physical or logical means. If physically separate test environments are not used, organizations determine the strength of mechanism required when implementing logical separation.

Related Controls: SA-11, SC-7.

(2) SECURITY AND PRIVACY IMPACT ANALYSES | VERIFICATION OF SECURITY AND PRIVACY FUNCTIONS

Check the security and privacy functions after system changes, to verify that the functions are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security and privacy requirements for the system.

Supplemental Guidance: Implementation in this context refers to installing changed code in the operational system.

Related Controls: SA-11, SC-3, SI-6.

References: NIST Special Publication 800-128.

CM-5 ACCESS RESTRICTIONS FOR CHANGE

Control: Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.

Supplemental Guidance: Any changes to the hardware, software, and/or firmware components of systems can potentially have significant effects on the overall security of the systems. Therefore, organizations permit only qualified and authorized individuals to access systems for purposes of initiating changes, including upgrades and modifications. ~~Organizations maintain records of access to ensure that configuration change control is implemented and to support after-the-fact actions should organizations discover any unauthorized changes.~~ Access restrictions for change also include software libraries. Access restrictions include, for example, physical and logical access controls (see AC-3 and PE-3), workflow automation, media libraries, abstract layers (i.e., changes implemented into ~~third-party~~external interfaces rather than directly into systems), and change windows (i.e., changes occur only during specified times~~, making unauthorized changes easy to discover).~~).

Related Controls: AC-3, AC-5, AC-6, CM-9, PE-3, SC-28, SC-34, SC-37, SI-2, SI-10.

Control Enhancements:

(1) ACCESS RESTRICTIONS FOR CHANGE | AUTOMATED ACCESS ENFORCEMENT AND AUDITING

(a) Enforce access restrictions; and

(b) Generate audit records of the enforcement actions.

Supplemental Guidance: Organizations log access records associated with applying configuration changes to ensure that configuration change control is implemented and to support after-the-fact actions should organizations discover any unauthorized changes.

Related Controls: AU-2, AU-6, AU-7, AU-12, CM-6, CM-11, SI-12.

(2) ACCESS RESTRICTIONS FOR CHANGE | REVIEW SYSTEM CHANGES

Review system changes [*Assignment: organization-defined frequency*] and [*Assignment: organization-defined circumstances*] to determine whether unauthorized changes have occurred.

Supplemental Guidance: Indications that warrant review of system changes and the specific circumstances justifying such reviews may be obtained from activities carried out by organizations during the configuration change process.

Related Controls: AU-6, AU-7, CM-3.

(3) ACCESS RESTRICTIONS FOR CHANGE | SIGNED COMPONENTS

Prevent the installation of [*Assignment: organization-defined software and firmware components*] without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

Supplemental Guidance: Software and firmware components prevented from installation unless signed with recognized and approved certificates include, for example, software and firmware version updates, patches, service packs, device drivers, and basic input output system (BIOS) updates. Organizations can identify applicable software and firmware components by type, by specific items, or a combination of both. Digital signatures and organizational verification of such signatures, is a method of code authentication.

Related Controls: CM-7, SC-13, SI-7.

(4) ACCESS RESTRICTIONS FOR CHANGE | DUAL AUTHORIZATION

Enforce dual authorization for implementing changes to [*Assignment: organization-defined system components and system-level information*].

Supplemental Guidance: Organizations employ dual authorization to ensure that any changes to selected system components and information cannot occur unless two qualified individuals implement such changes. The two individuals possess sufficient skills and expertise to determine if the proposed changes are correct implementations of approved changes. Dual authorization may also be known as two-person control.

Related Controls: AC-2, AC-5, CM-3.

(5) ACCESS RESTRICTIONS FOR CHANGE | ~~*LIMIT*~~PRIVILEGE LIMITATION FOR PRODUCTION ~~/ *OPERATIONAL PRIVILEGES*~~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*].

Supplemental Guidance: In many organizations, systems support many missions and business functions. Limiting privileges to change system components with respect to operational systems is necessary because changes to a ~~particular information~~ system component may have far-reaching effects on mission and business processes supported by the system ~~where the component resides~~. The complex, many-to-many relationships between systems and mission/business processes are in some cases, unknown to developers.

Related Controls: AC-2.

(6) ACCESS RESTRICTIONS FOR CHANGE | LIMIT LIBRARY PRIVILEGES

Limit privileges to change software resident within software libraries.

Supplemental Guidance: Software libraries include privileged programs.

Related Controls: AC-2.

(7) ACCESS RESTRICTIONS FOR CHANGE | AUTOMATIC IMPLEMENTATION OF SECURITY SAFEGUARDS

[Withdrawn: Incorporated into SI-7].

References: FIPS Publications 140-2, 186-4.

CM-6 CONFIGURATION SETTINGS

Control:

a. Establish and document configuration settings for components employed within the system using [*Assignment: organization-defined* ~~*security configuration checklists*~~*common secure configurations*] that reflect the most restrictive mode consistent with operational requirements;

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.

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

Common secure configurations (also referred to as security configuration checklists, lockdown and hardening guides, security reference guides, security technical implementation guides) provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for specific information technology platforms/products and instructions for configuring those system components to meet operational requirements. Common secure configurations can be developed by a variety of organizations including, for example, information technology product developers, manufacturers, vendors, consortia, academia, industry, federal agencies, and other organizations in the public and private sectors. Implementation of a specific common secure configuration may be mandated at the organizational or mission/business process level or may be mandated at a higher level including, for example, by a regulatory agency. Common secure configurations include the United States Government Configuration Baseline (USGCB) which affects the implementation of CM-6 and other controls such as AC-19 and CM-7. The Security Content Automation Protocol (SCAP) and the defined standards within the protocol ~~(e.g., Common Configuration Enumeration)~~ provide an effective method to uniquely identify, track, and control configuration settings~~. OMB establishes federal policy on configuration requirements for federal information systems~~.

Related Controls: 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, RA-5, SA-4, SA-5, SA-9, SC-18, SC-19, SC-28, SC-43, SI-2, SI-4, SI-6.

Control Enhancements:

(1) CONFIGURATION SETTINGS | AUTOMATED ~~*CENTRAL*~~ MANAGEMENT, APPLICATION, AND VERIFICATION

Employ automated mechanisms to centrally manage, apply, and verify configuration settings for [*Assignment: organization-defined system components*].

Supplemental Guidance:

Related Controls: CA-7.

(2) CONFIGURATION SETTINGS | RESPOND TO UNAUTHORIZED CHANGES

Employ [*Assignment: organization-defined security safeguards*] to respond to unauthorized changes to [*Assignment: organization-defined configuration settings*].

Supplemental Guidance: Responses to unauthorized changes to configuration settings can include, for example, alerting designated organizational personnel, restoring established configuration settings, or in extreme cases, halting affected system processing.

Related Controls: IR-4, IR-6, SI-7.

(3) CONFIGURATION SETTINGS | UNAUTHORIZED CHANGE DETECTION

[Withdrawn: Incorporated into SI-7].

(4) CONFIGURATION SETTINGS | CONFORMANCE DEMONSTRATION

[Withdrawn: Incorporated into CM-4].

References: NIST Special Publications 800-70, 800-126, 800-128; US Government Configuration Baselines; National Checklist Repository.

CM-7 LEAST FUNCTIONALITY

Control:

a. Configure the system to provide only essential capabilities; and

b. Prohibit or restrict the use of the following functions, ports, protocols, and/or services: [*Assignment: organization-defined prohibited or restricted functions, ports, protocols, and/or services*].

Supplemental Guidance: Systems provide a wide variety of functions and services. Some of the functions and services routinely provided by default, may not be necessary to support essential organizational ~~operations (e.g., key~~ missions, functions, or operations. Additionally, it is sometimes convenient to provide multiple services from a single system component, but doing so increases risk over limiting the services provided by that single component. Where feasible, organizations limit component functionality to a single function per ~~device (e.g., email servers or web servers, but not both).~~component. Organizations review functions and services provided by systems or ~~individual~~ components of systems, to determine which functions and services are candidates for elimination ~~(e.g., .Voice Over Internet Protocol, Instant Messaging, auto-execute, and file sharing).~~ Organizations consider disabling unused or unnecessary physical and logical ports~~/~~ and protocols ~~(e.g., Universal Serial Bus, File Transfer Protocol, and Hyper Text Transfer Protocol) on information systems~~ to prevent unauthorized connection of devices, ~~unauthorized~~ transfer of information, ~~or unauthorized~~ and tunneling. Organizations employ network scanning tools, intrusion detection and prevention systems, and end-point protection technologies such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, protocols, ports, and services.

Related Controls: AC-3, AC-4, CM-2, CM-5, CM-11, RA-5, SA-4, SA-5, SA-9, SA-15, SC-7, SC-37. SI-4.

Control Enhancements:

(1) LEAST FUNCTIONALITY | PERIODIC REVIEW

(a) Review the system [*Assignment: organization-defined frequency*] to identify unnecessary and/or nonsecure functions, ports, protocols, and services; and

(b) Disable [*Assignment: organization-defined functions, ports, protocols, and services within the system deemed to be unnecessary and/or nonsecure*].

Supplemental Guidance: Organizations can either decide the relative security of the function, port, protocol, and/or service or base the security decision on the assessment of other entities. Bluetooth, FTP, and peer-to-peer networking are examples of less than secure protocols.

Related Controls: AC-18.

(2) LEAST FUNCTIONALITY | PREVENT PROGRAM EXECUTION

Prevent program execution in accordance with [*Selection (one or more):* [*Assignment: organization-defined policies regarding software program usage and restrictions*]*; rules authorizing the terms and conditions of software program usage*].

Supplemental Guidance: This control enhancement addresses organizational policies restricting software usage as well as the terms and conditions imposed by the developer or manufacturer including, for example, software licensing and copyrights. Restrictions include, for example, restricting the roles allowed to approve program execution; prohibiting auto-execute; program blacklisting and whitelisting; or restricting the number of program instances executed at the same time.

Related Controls: CM-8, PM-5.

(3) LEAST FUNCTIONALITY | REGISTRATION COMPLIANCE

Ensure compliance with [*Assignment: organization-defined registration requirements for functions, ports, protocols, and services*].

Supplemental Guidance: Organizations use the registration process to manage, track, and provide oversight for systems and implemented functions, ports, protocols, and services.

Related Controls: None.

(4) LEAST FUNCTIONALITY | UNAUTHORIZED SOFTWARE — BLACKLISTING

(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*].

Supplemental Guidance: The process used to identify specific software programs or entire categories of software programs that are not authorized to execute on organizational ~~information~~ systems is commonly referred to as *blacklisting*. Organizations can implement CM-7(5) instead of this control enhancement if whitelisting (the stronger of the two policies) is the preferred approach for restricting software program execution.

Related Controls: CM-6, CM-8, CM-10, PM-5.

(5) LEAST FUNCTIONALITY | AUTHORIZED SOFTWARE — WHITELISTING

(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*].

Supplemental Guidance: The process used to identify specific software programs or entire categories of software programs that are authorized to execute on organizational systems is commonly referred to as *whitelisting*. To effect comprehensive whitelisting and increase the strength of protection for attacks that bypass application level whitelisting, software programs may be decomposed into and monitored at multiple levels of detail. Software program levels of detail include, for example, applications, application programming interfaces, application modules, scripts, system processes, system services, kernel actions, registries, drivers, and dynamic link libraries. The concept of whitelisting may also be applied to user actions, ports, IP addresses, and media access control (MAC) addresses. Organizations consider verifying the integrity of white-listed software programs using, for example, cryptographic checksums, digital signatures, or hash functions. Verification of white-listed software can occur either prior to execution or at system startup.

Related Controls: CM-2, CM-6, CM-8, CM-10, PM-5, SA-10, SC-34, SI-7.

References: FIPS Publications 140-2, 180-4, 186-4, 202; NIST Special Publication 800-167.

CM-8 SYSTEM COMPONENT INVENTORY

Control:

a. Develop and document an inventory of system components that:

   1. Accurately reflects the current system;

   2. Includes all components within the authorization boundary of the system;

   3. Is at the level of granularity deemed necessary for tracking and reporting; and

   4. Includes [*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*].

Supplemental Guidance: System components are discrete identifiable information technology assets that represent a building block of a system and include hardware, software, firmware, and virtual

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

Related Controls: CM-2, CM-7, CM-9, CM-10, CM-11, CP-2, CP-9, MA-6, PE-20, PM-5, PM-29, SA-4, SA-5, SI-2.

Control Enhancements:

(1) SYSTEM COMPONENT INVENTORY | UPDATES DURING INSTALLATION AND REMOVAL

Update the inventory of system components as an integral part of component installations, removals, and system updates.

Supplemental Guidance: None.

Related Controls: None.

(2) SYSTEM COMPONENT INVENTORY | AUTOMATED MAINTENANCE

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

Supplemental Guidance: Organizations maintain system inventories to the extent feasible. Virtual machines, for example, 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. This control enhancement can be satisfied by the implementation of CM-2 (2) for organizations that choose to combine system component inventory and baseline configuration activities.

Related Controls: None.

(3) SYSTEM COMPONENT INVENTORY | AUTOMATED UNAUTHORIZED COMPONENT DETECTION

(a) Employ automated mechanisms [*Assignment: organization-defined frequency*] to detect the presence of unauthorized hardware, software, and firmware components within the system; 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*]].

Supplemental Guidance: This control enhancement is applied in addition to the monitoring for unauthorized remote connections and mobile devices. Monitoring for unauthorized system components may be accomplished on an ongoing basis or by the periodic scanning of systems for that purpose. Automated mechanisms can be implemented within systems or in other separate devices. Isolation can be achieved, for example, by placing unauthorized system components in separate domains or subnets or otherwise quarantining such components. This type of component isolation is commonly referred to as sandboxing.

Related Controls: AC-19, CA-7, RA-5, SI-3, SI-4, SI-7.

(4) SYSTEM COMPONENT INVENTORY | ACCOUNTABILITY INFORMATION

Includes in the system component inventory information, a means for identifying by [*Selection (one or more): name; position; role*], individuals responsible and accountable for administering those components.

Supplemental Guidance: Identifying individuals who are both responsible and accountable for administering system components helps to ensure that the assigned components are properly administered and organizations can contact those individuals if some action is required, for example, the component is determined to be the source of a breach ~~/compromise~~; the component needs to be recalled or replaced; or the component needs to be relocated.

Related Controls: None.

(5) SYSTEM COMPONENT INVENTORY | NO DUPLICATE ACCOUNTING OF COMPONENTS

(a) Verify that all components within the authorization boundary of the system are not duplicated in other system component inventories; or

~~(a)~~(b) If a centralized component inventory is used, verify components are not assigned to multiple systems.

Supplemental Guidance: This control enhancement addresses the potential problem of duplicate accounting of system components in large or complex interconnected systems.

Related Controls: None.

(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.

Supplemental Guidance: This control enhancement focuses 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.

Related Controls: None.

(7) SYSTEM COMPONENT INVENTORY | CENTRALIZED REPOSITORY

Provide a centralized repository for the inventory of system components.

Supplemental Guidance: Organizations may choose to implement centralized system component inventories that include components from all organizational systems. Centralized repositories of system 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 system 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.

Related Controls: None.

(8) SYSTEM COMPONENT INVENTORY | AUTOMATED LOCATION TRACKING

Employ automated mechanisms to support tracking of system components by geographic location.

Supplemental Guidance: The use of automated mechanisms to track the location of system components can increase the accuracy of component inventories. Such capability may also 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.

Related Controls: None.

(9) SYSTEM COMPONENT INVENTORY | ASSIGNMENT OF COMPONENTS TO SYSTEMS

(a) Assign [*Assignment: organization-defined acquired system components*] to a system; and

(b) Receive an acknowledgement from ~~the system owner~~[*Assignment: organization-defined personnel or roles*] of this assignment.

Supplemental Guidance: Organizations determine the ~~criteria for or~~ types of system components ~~(e.g., microprocessors, motherboards, software, programmable logic controllers, and network devices)~~ that are subject to this control enhancement.

Related Controls: None.

(10) SYSTEM COMPONENT INVENTORY | DATA ACTION MAPPING

Develop and document a system map of data actions that process personally identifiable information.

Supplemental Guidance: Data actions are system operations that process personally identifiable information. Such processing encompasses the full information life cycle which includes collection, generation, transformation, use, disclosure, retention, disposal. Creating a system map of data actions supports a privacy risk assessment. The development of this map may

necessitate coordination between the privacy and security programs regarding the covered data actions, the system components, and the definition of the authorization boundary.

Related Controls: PM-30, CM-4.

References: NIST Special Publications 800-57-1, 800-57-2, 800-57-3, 800-128; NIST Interagency Report 8062.

CM-9 CONFIGURATION MANAGEMENT PLAN

Control: 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

~~d.~~e. Protects the configuration management plan from unauthorized disclosure and modification.

Supplemental Guidance: Configuration management plans satisfy the requirements in configuration management policies while being tailored to individual systems. Such plans define ~~detailed~~ processes and procedures for how configuration management is used to support system development life cycle activities ~~at the information system level.~~. Configuration management plans are typically developed during the development and acquisition phase of the system development life cycle. The plans describe how to move changes through change management processes, how to update configuration settings and baselines, how to maintain system component inventories, how to control development, test, and operational environments, and how to develop, release, and update key documents. Organizations can employ templates to help ensure consistent and timely development and implementation of configuration management plans. Such templates can represent a master configuration management plan for the organization ~~at large~~ with subsets of the plan implemented on a system by system basis. Configuration management approval processes include designation of key management stakeholders responsible for reviewing and approving proposed changes to systems, and personnel that conduct security impact analyses prior to the implementation of changes to the systems. Configuration items are the system ~~items~~ (components (i.e., 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.

Related Controls: CM-2, CM-3, CM-4, CM-5, CM-8, PL-2, SA-10, SI-12.

Control Enhancements:

(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.

Supplemental Guidance: In the absence of dedicated configuration management teams assigned within organizations, system developers may be tasked to develop configuration management processes using personnel who are not directly involved in system development or 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.

Related Controls: None.

References: NIST Special Publication 800-128.

CM-10 SOFTWARE USAGE RESTRICTIONS

Control:

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.

Supplemental Guidance: Software license tracking can be accomplished by manual methods ~~(e.g., simple spreadsheets)~~ or automated methods ~~(e.g., specialized tracking applications)~~ depending on organizational needs.

Related Controls: AC-17, AU-6, CM-7, CM-8, SC-7.

Control Enhancements:

(1) SOFTWARE USAGE RESTRICTIONS | OPEN SOURCE SOFTWARE

Establish the following restrictions on the use of open source software: [*Assignment: organization-defined restrictions*].

Supplemental Guidance: Open source software refers to software that is available in source code form. Certain software rights normally reserved for copyright holders are routinely provided under software license agreements that permit individuals to study, change, and improve the software. From a security perspective, the major advantage of open source software is that it provides organizations with the ability to examine the source code. However, there are also various licensing issues associated with open source software including, for example, the constraints on derivative use of such software.

Related Controls: SI-7.

References: None.

CM-11 USER-INSTALLED SOFTWARE

Control:

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 at [*Assignment: organization-defined frequency*].

Supplemental Guidance: If provided the necessary privileges, users have the ability to install software in organizational systems. To maintain control over the types of software installed, organizations identify permitted and prohibited actions regarding software installation. Permitted software installations may include, for example, updates and security patches to existing software and downloading applications from organization-approved "app stores." Prohibited software installations may include, for example, software with unknown or suspect pedigrees or software that organizations consider potentially malicious. The policies organizations select governing user-installed software may be organization-developed or provided by some external entity. Policy enforcement methods include procedural methods ~~(e.g., periodic examination of user accounts), automated methods (e.g., configuration settings implemented on organizational information systems), or both.~~, automated methods, or both.

Related Controls: AC-3, AU-6, CM-2, CM-3, CM-5, CM-6, CM-7, CM-8, PL-4, SI-7.

Control Enhancements:

(1) USER-INSTALLED SOFTWARE | ALERTS FOR UNAUTHORIZED INSTALLATIONS

~~**The information system alerts [*Assignment: organization-defined personnel or roles*] when the unauthorized**~~[Withdrawn: Incorporated into CM-8(3)].

(2) SOFTWARE INSTALLATION WITH PRIVILEGED STATUS

Allow user installation of software ~~is detected.~~

~~**a.** *USER-INSTALLED SOFTWARE | PROHIBIT INSTALLATION WITHOUT PRIVILEGED STATUS*~~

~~The information system prohibits user installation of software without~~only with explicit privileged status.

Supplemental Guidance: Privileged status can be obtained, for example, by serving in the role of system administrator.

Related Controls: AC-5, AC-6.

References: None.

CM-12 INFORMATION LOCATION

Control:

a. Identify the location of [*Assignment: organization-defined information*] and the specific system components on which the information resides;

b. Identify and document the users who have access to the system and system components where the information resides; and

c. Document changes to the location (i.e., system or system components) where the information resides.

Supplemental Guidance: This control addresses the need to understand where information is being processed and stored and is typically applied with respect to Controlled Unclassified Information (CUI). The National Archives and Records Administration defines the types of information that are categorized as CUI. Information location includes identifying where specific information types and associated information reside in the system components that compose organizational systems; and how information is being processed so that information flow can be understood and adequate protection and policy management provided for such information and system components.

Related Controls: AC-3, AC-4, AC-6, AC-23, CM-8, PM-29, SC-4, SC-16, SC-28, SI-4, SI-7.

Control Enhancements:

(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 adequate security and privacy controls are in place to protect organizational information and individual privacy.

Supplemental Guidance: This control enhancement gives organizations the capability to check systems and selected system components for types of information to confirm such information resides on the component and to ensure that the required protection measures are in place for that component.

Related Controls: None.

References: FIPS Publication 199; NIST Special Publication 800-60-1, 800-60-2.

3.6 CONTINGENCY PLANNING

Quick link to Contingency Planning summary table

CP-1 CONTINGENCY PLANNING POLICY AND PROCEDURES

Control:

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

1. A 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 senior management official*] to manage the contingency planning policy and procedures;

~~b.~~c. Review and update the current contingency planning:

1. Policy [*Assignment: organization-defined frequency*]; and

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

d. Ensure that the contingency planning procedures implement the contingency planning policy and controls; and

e. Develop, document, and implement remediation actions for violations of the contingency planning policy.

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of ~~selected security~~ the controls and control enhancements in the CP family. The risk management strategy is an important factor in establishing policy and procedures ~~reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security~~. Comprehensive policy and procedures help provide security and privacy assurance. Security and privacy program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general ~~information~~ security and privacy policy ~~for organizations or conversely,~~or can be represented by multiple policies reflecting the complex nature of ~~certain~~ organizations. The procedures can be established for ~~the~~ security ~~program in general~~and privacy programs and for ~~particular information~~ systems, if needed. ~~The~~Procedures describe how policies or controls are implemented and can be directed at the personnel 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. It is important to recognize that restating controls does not constitute an organizational ~~risk management strategy is a key factor in establishing~~ policy ~~and procedures.~~ or procedure.

Related Controls: PM-9, PS-8, SI-12.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-30, 800-34, 800-39, 800-100.

CP-2 CONTINGENCY PLAN

Control:

a. Develop a contingency plan for the system that:

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

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

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

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

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

6. Is reviewed and approved by [*Assignment: organization-defined personnel or roles*];

b. Distributes copies of the contingency plan to [*Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements*];

c. Coordinates contingency planning activities with incident handling activities;

d. Reviews the contingency plan for the system [*Assignment: organization-defined frequency*];

e. Updates 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. Communicates contingency plan changes to [*Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements*]; and

g. Protects the contingency plan from unauthorized disclosure and modification.

Supplemental Guidance: Contingency planning for systems is part of an overall organizational program for achieving continuity of operations for mission/business functions. Contingency planning addresses system restoration and implementation of alternative mission or business processes when systems are compromised or breached. The effectiveness of contingency planning is maximized by considering such planning throughout the ~~phases of the~~ system development life cycle. Performing contingency planning on hardware, software, and firmware development can be an effective means of achieving system resiliency. 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, policies, standards, regulations, and guidelines. In addition to ~~system~~ availability, contingency plans address other security-related events resulting in a reduction in mission or business effectiveness, such as malicious attacks compromising the confidentiality or integrity of systems. Actions addressed in contingency plans include, for example, orderly and graceful 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 can ensure that the necessary planning activities are in place and activated in the event of a security incident.

Related Controls: 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.

Control Enhancements:

(1) CONTINGENCY PLAN | COORDINATE WITH RELATED PLANS

Coordinate contingency plan development with organizational elements responsible for related plans.

Supplemental Guidance: Plans related to contingency plans for organizational systems include, for example, Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, Insider Threat Implementation Plan, and Occupant Emergency Plans.

Related Controls: None.

(2) CONTINGENCY PLAN | CAPACITY PLANNING

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

Supplemental Guidance: Capacity planning is needed because different types of threats ~~(e.g., natural disasters, targeted cyber attacks)~~ can result in a reduction of the available processing, telecommunications, and support services ~~originally~~ intended to support the organizational missions and business functions. Organizations need to anticipate degraded operations during contingency operations and factor such degradation into capacity planning. With respect to capacity planning, environmental support refers to any environmental support factor for which the organization determines that it needs to provide support in a contingency situation, even if in a degraded state. As always, such determinations are based on an assessment of risk, system categorization (impact level), and organizational risk tolerance.

Related Controls: PE-11, PE-12, PE-13, PE-14, PE-18, SC-5.

(3) CONTINGENCY PLAN | RESUME ESSENTIAL MISSIONS AND BUSINESS FUNCTIONS

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

Supplemental Guidance: Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. The time-period for resumption of essential missions and business functions may be dependent on the severity and extent of the disruptions to the system and its supporting infrastructure.

Related Controls: None.

(4) CONTINGENCY PLAN | RESUME ALL MISSIONS AND BUSINESS FUNCTIONS

~~**The organization plans for the continuance of essential missions and business functions with little or no loss of operational continuity and sustains that continuity until full information system restoration at primary processing and/or storage sites.**~~ **Plan for the resumption of all missions and business functions within [*Assignment: organization-defined time -period*] of contingency plan activation.**

Supplemental Guidance: Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of 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 (e.g., backup sites may become primary sites).~~ The time-period for resumption of missions and business functions may be dependent on the severity and extent of disruptions to the system and its supporting infrastructure.

Related Controls: None.

(5) CONTINGENCY PLAN | CONTINUE ESSENTIAL MISSIONS AND BUSINESS FUNCTIONS

Plan for the continuance of essential missions and business functions with little or no loss of operational continuity and sustains that continuity until full system restoration at primary processing and/or storage sites.

Supplemental Guidance: Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of 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.

Related Controls: None.

~~(5)~~(6) CONTINGENCY PLAN | ALTERNATE PROCESSING AND STORAGE SITE

Plan for the transfer of essential missions and business functions to alternate processing and/or storage sites with little or no loss of operational continuity and sustain that continuity through system restoration to primary processing and/or storage sites.

Supplemental Guidance: Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning

including, for example, as part of 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 ~~(e.g., backup sites may become primary sites).~~

Related Controls: None.

~~(6)~~(7) CONTINGENCY PLAN | COORDINATE WITH EXTERNAL SERVICE PROVIDERS

Coordinate the contingency plan with the contingency plans of external service providers to ensure that contingency requirements can be satisfied.

Supplemental Guidance: When the capability of an organization to successfully carry out its core missions and business functions is dependent on external service providers, developing a timely and comprehensive contingency plan may become more challenging. In this situation, organizations coordinate contingency planning activities with the external entities to ensure that the individual plans reflect the overall contingency needs of the organization.

Related Controls: SA-9.

~~(7)~~(8) CONTINGENCY PLAN | IDENTIFY CRITICAL ASSETS

Identify critical system assets supporting essential missions and business functions.

Supplemental Guidance: Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational criticality analysis or business continuity planning including, for example, as part of business impact analyses. Organizations identify critical ~~information~~ system assets so ~~that~~ additional safeguards and countermeasures can be employed (beyond those safeguards and countermeasures routinely implemented) to help ensure that organizational missions/business functions can continue to be conducted during contingency operations. The identification of critical information assets also facilitates the prioritization of organizational resources. Critical system assets include both technical and operational aspects. Technical aspects include, for example, information technology services, system components, information technology products, and mechanisms. Operational aspects include, for example, procedures (manually executed operations) and personnel (individuals operating technical safeguards and/or executing manual procedures). Organizational program protection plans can aid in identifying critical assets.

Related Controls: CM-8, RA-9.

References: NIST Special Publication 800-34; NIST Interagency Report 8179.

CP-3 CONTINGENCY TRAINING

Control: Provide contingency training to system users consistent with assigned roles and responsibilities:

a. Within [*Assignment: organization-defined time period*] of assuming a contingency role or responsibility;

b. When required by system changes; and

c. [*Assignment: organization-defined frequency*] thereafter.

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

Related Controls: AT-2, AT-3, AT-4, CP-2, CP-4, CP-8, IR-2, IR-4, IR-9.

Control Enhancements:

(1) CONTINGENCY TRAINING | SIMULATED EVENTS

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

Supplemental Guidance: None.

Related Controls: None.

(2) CONTINGENCY TRAINING | AUTOMATED TRAINING ENVIRONMENTS

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

Supplemental Guidance: None.

Related Controls: None.

References: NIST Special Publication 800-50.

CP-4 CONTINGENCY PLAN TESTING

Control:

a. Test the contingency plan for the system [*Assignment: organization-defined frequency*] using [*Assignment: organization-defined tests*] to determine the effectiveness of the plan and the organizational readiness to execute the plan;

b. Review the contingency plan test results; and

c. Initiate corrective actions, if needed.

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

Related Controls: AT-3, CP-2, CP-3, CP-8, CP-9, IR-3, IR-4, PL-2, PM-14.

Control Enhancements:

(1) CONTINGENCY PLAN TESTING | COORDINATE WITH RELATED PLANS

Coordinate contingency plan testing with organizational elements responsible for related plans.

Supplemental Guidance: Plans related to contingency plans for organizational systems include, for example, business continuity plans, disaster recovery plans, continuity of operations plans, crisis communications plans, critical infrastructure plans, cyber incident response plans, and occupant emergency plans. This control enhancement does not require organizations to create organizational elements to handle related plans or to align such elements with specific plans. It does require, however, that if such organizational elements are responsible for related plans, organizations should coordinate with those elements.

Related Controls: IR-8, PM-8.

(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.

Supplemental Guidance: None.

Related Controls: CP-7.

(3) CONTINGENCY PLAN TESTING | AUTOMATED TESTING

Employ automated mechanisms to more thoroughly and effectively test the contingency plan.

Supplemental Guidance: Automated mechanisms facilitate more thorough and effective testing of contingency plans. This occurs by providing more complete coverage of contingency issues; by selecting more realistic test scenarios and environments; and by effectively stressing the system and supported missions and business operations.

Related Controls: None.

(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 plan testing.

Supplemental Guidance: None.

Related Controls: CP-10, SC-24.

References: FIPS Publication 199; NIST Special Publications 800-34, 800-84.

CP-5 CONTINGENCY PLAN UPDATE

[Withdrawn: Incorporated into CP-2].

CP-6 ALTERNATE STORAGE SITE

Control:

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 security controls equivalent to that of the primary site.

Supplemental Guidance: Alternate storage sites are sites that are geographically distinct from primary storage sites. An alternate storage site maintains duplicate copies of information and data if the primary storage site is not available. Items covered by alternate storage site agreements include, for example, environmental conditions at alternate sites, access rules, physical and environmental protection requirements, and coordination of delivery/retrieval of backup media. Alternate storage sites reflect the requirements in contingency plans so that organizations can maintain essential missions and business functions despite disruption, compromise, or failure in organizational systems.

Related Controls: CP-2, CP-7, CP-8, CP-9, CP-10, MP-4, MP-5, PE-3, SC-36, SI-13.

Control Enhancements:

(1) ALTERNATE STORAGE SITE | SEPARATION FROM PRIMARY SITE

Identify an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.

Supplemental Guidance: Threats that affect alternate storage sites are ~~typically~~ defined in organizational assessments of risk and include, for example, natural disasters, structural failures, hostile ~~cyber~~ attacks, and errors of omission or commission. Organizations determine what is considered a sufficient degree of separation between primary and alternate storage sites based on the types of threats that are of concern. For ~~one particular type of threat (i.e.,~~threats such as hostile ~~cyber attack),~~attacks, the degree of separation between sites is less relevant.

Related Controls: RA-3.

(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.

Supplemental Guidance: None.

Related Controls: None.

(3) ALTERNATE STORAGE SITE | ACCESSIBILITY

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

Supplemental Guidance: Area-wide disruptions refer to those types of disruptions that are broad in geographic scope ~~(e.g., hurricane, regional power outage)~~ with such determinations made by organizations based on organizational assessments of risk. Explicit mitigation actions include, for example, duplicating backup information at other alternate storage sites if access problems occur at originally designated alternate sites; or planning for physical access to retrieve backup information if electronic accessibility to the alternate site is disrupted.

Related Controls: RA-3.

References: NIST Special Publication 800-34.

CP-7 ALTERNATE PROCESSING SITE

Control:

a. Establish an alternate processing site including necessary agreements to permit the transfer and resumption of [*Assignment: organization-defined system operations*] for essential missions 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 information security and privacy safeguards at the alternate processing site that are equivalent to those at the primary site.

Supplemental Guidance: Alternate processing sites are sites that are geographically distinct from primary processing sites. An alternate processing site provides processing capability if the primary processing site is not available. ~~Items~~Geographically distributed architectures may also be considered as alternate processing sites. Safeguards that are covered by alternate processing site agreements include, for example, environmental conditions at alternate sites; access rules; physical and environmental protection requirements; and the coordination for the transfer and assignment of personnel. Requirements are specifically allocated to alternate processing sites that reflect the requirements in contingency plans to maintain essential missions and business functions despite disruption, compromise, or failure in organizational systems.

Related Controls: CP-2, CP-6, CP-8, CP-9, CP-10, MA-6, PE-3, PE-11, PE-12, PE-17, SC-36, SI-13.

Control Enhancements:

(1) ALTERNATE PROCESSING SITE | SEPARATION FROM PRIMARY SITE

Identify an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.

Supplemental Guidance: Threats that affect alternate processing sites are typically defined in organizational assessments of risk and include, for example, natural disasters, structural failures, hostile ~~cyber~~ attacks, and errors of omission/commission. Organizations determine what is considered a sufficient degree of separation between primary and alternate processing sites based on the types of threats that are of concern. For ~~one particular type of threat (i.e.,~~threats such as hostile ~~cyber attack),~~attacks, the degree of separation between sites is less relevant.

Related Controls: RA-3.

(2) ALTERNATE PROCESSING SITE | ACCESSIBILITY

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

Supplemental Guidance: Area-wide disruptions refer to those types of disruptions that are broad in geographic scope ~~(e.g., hurricane, regional power outage)~~ with such determinations made by organizations based on organizational assessments of risk.

Related Controls: RA-3.

(3) ALTERNATE PROCESSING SITE | PRIORITY OF SERVICE

Develop alternate processing site agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives).

Supplemental Guidance: 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 at the alternate processing site.

Related Controls: None.

(4) ALTERNATE PROCESSING SITE | PREPARATION FOR USE

Prepare the alternate processing site so that the site is ready to be used as the operational site supporting essential missions and business functions.

Supplemental Guidance: Site preparation includes, for example, establishing configuration settings for system components at the alternate processing site consistent with the requirements for such settings at the primary site and ensuring that essential supplies and other logistical considerations are in place.

Related Controls: CM-2, CM-6, CP-4.

(5) ALTERNATE PROCESSING SITE | EQUIVALENT INFORMATION SECURITY SAFEGUARDS

[Withdrawn: Incorporated into 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.

Supplemental Guidance: None.

Related Controls: None.

References: NIST Special Publication 800-34.

CP-8 TELECOMMUNICATIONS SERVICES

Control: Establish alternate telecommunications services including necessary agreements to permit the resumption of [*Assignment: organization-defined system operations*] for essential missions and business functions within [*Assignment: organization-defined time-period*] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

Supplemental Guidance: This control applies to telecommunications services (data and voice) for primary and alternate processing and storage sites. Alternate telecommunications services reflect the continuity requirements in contingency plans to maintain essential missions and business functions despite the loss of primary telecommunications services. Organizations may specify different time-periods for primary/alternate sites. Alternate telecommunications services include, for example, additional organizational or commercial ground-based circuits/lines or satellites in lieu of ground-based communications. Organizations consider factors such as availability, quality of service, and access when entering alternate telecommunications agreements.

Related Controls: CP-2, CP-6, CP-7, CP-11, SC-7.

Control Enhancements:

(1) TELECOMMUNICATIONS SERVICES | PRIORITY OF SERVICE PROVISIONS

(a) Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives); and

(b) Request Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness ~~in the event that~~if the primary and/or alternate telecommunications services are provided by a common carrier.

Supplemental Guidance: Organizations consider the potential mission/business impact in situations where telecommunications service providers are servicing other organizations with similar priority-of-service provisions.

Related Controls: None.

(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.

Supplemental Guidance: None.

Related Controls: None.

(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.

Supplemental Guidance: Threats that affect telecommunications services are typically defined in organizational assessments of risk and include, for example, natural disasters, structural failures, hostile cyber/physical attacks, and errors of omission/commission. Organizations seek to reduce common susceptibilities by, for example, 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 meeting the separation needs addressed in the risk assessment.

Related Controls: None.

(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*].

Supplemental Guidance: Reviews of provider contingency plans consider the proprietary nature of such plans. In some situations, a summary of provider contingency plans may be sufficient evidence for organizations to satisfy the review requirement. Telecommunications service providers may also participate in ongoing disaster recovery exercises in coordination with the Department of Homeland Security, state, and local governments. Organizations may use these types of activities to satisfy evidentiary requirements related to service provider contingency plan reviews, testing, and training.

Related Controls: CP-3, CP-4.

(5) TELECOMMUNICATIONS SERVICES | ALTERNATE TELECOMMUNICATION SERVICE TESTING

Test alternate telecommunication services [*Assignment: organization-defined frequency*].

Supplemental Guidance: CP-3.

Related Controls: None.

References: NIST Special Publication 800-34.

CP-9 SYSTEM BACKUP

Control:

a. Conduct backups of user-level information contained in the system [*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-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 at storage locations.

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

Related Controls: CP-2, CP-6, CP-10, MP-4, MP-5, SC-13, SI-4, SI-13.

Control Enhancements:

(1) SYSTEM BACKUP | TESTING FOR RELIABILITY AND INTEGRITY

Test backup information [*Assignment: organization-defined frequency*] to verify media reliability and information integrity.

Supplemental Guidance: None.

Related Controls: CP-4.

(2) SYSTEM BACKUP | TEST RESTORATION USING SAMPLING

Use a sample of backup information in the restoration of selected system functions as part of contingency plan testing.

Supplemental Guidance:

Related Controls: CP-4.

(3) SYSTEM BACKUP | SEPARATE STORAGE FOR CRITICAL INFORMATION

Store backup copies of [*Assignment: organization-defined critical system software and other security-related information*] in a separate facility or in a fire-rated container that is not collocated with the operational system.

Supplemental Guidance: Critical system software includes, for example, operating systems, cryptographic key management systems, and intrusion detection/prevention systems. Security-related information includes, for example, organizational inventories of hardware, software, and firmware components. Alternate storage sites typically serve as separate storage facilities for organizations.

Related Controls: CM-2, CM-6, CM-8.

(4) SYSTEM BACKUP | PROTECTION FROM UNAUTHORIZED MODIFICATION

[Withdrawn: Incorporated into CP-9].

(5) SYSTEM BACKUP | TRANSFER TO ALTERNATE STORAGE SITE

Transfer system backup information to the alternate storage site [*Assignment: organization-defined time-period and transfer rate consistent with the recovery time and recovery point objectives*].

Supplemental Guidance: System backup information can be transferred to alternate storage sites either electronically or by physical shipment of storage media.

Related Controls: CP-7, MP-3, MP-4, MP-5.

(6) SYSTEM BACKUP | REDUNDANT SECONDARY SYSTEM

Conduct system backup by maintaining a redundant secondary system that is not collocated with the primary system and that can be activated without loss of information or disruption to operations.

Supplemental Guidance:

Related Controls: CP-7.

(7) SYSTEM BACKUP | DUAL AUTHORIZATION

Enforce dual authorization for the deletion or destruction of [*Assignment: organization-defined backup information*].

Supplemental Guidance: Dual authorization ensures that the deletion or destruction of backup information cannot occur unless two qualified individuals carry out the task. Individuals deleting/destroying backup information possess sufficient skills/expertise to determine if the proposed deletion/destruction of backup information reflects organizational policies and procedures. Dual authorization may also be known as two-person control.

Related Controls: AC-3, AC-5, MP-2.

(8) SYSTEM BACKUP | CRYPTOGRAPHIC PROTECTION

Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of [*Assignment: organization-defined backup information*].

Supplemental Guidance: The selection of cryptographic mechanisms is based on the need to protect the confidentiality and integrity of backup information. The strength of mechanism is commensurate with the security category and/or classification of the information. This control enhancement applies to system backup information in storage at primary and alternate locations. Organizations implementing cryptographic mechanisms to protect information at rest also consider cryptographic key management solutions.

Related Controls: SC-12, SC-13, SC-28.

References: FIPS Publications 140-2, 186-4; NIST Special Publications 800-34, 800-130, 800-152.

CP-10 SYSTEM RECOVERY AND RECONSTITUTION

Control: Provide for the recovery and reconstitution of the system to a known state after a disruption, compromise, or failure within [*Assignment: organization-defined time-period consistent with recovery time and recovery point objectives*].

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

Related Controls: CP-2, CP-4, CP-6, CP-7, CP-9, IR-4, SC-24, SI-13.

Control Enhancements:

(1) SYSTEM RECOVERY AND RECONSTITUTION | CONTINGENCY PLAN TESTING

[Withdrawn: Incorporated into CP-4].

(2) SYSTEM RECOVERY AND RECONSTITUTION | TRANSACTION RECOVERY

Implement transaction recovery for systems that are transaction-based.

Supplemental Guidance: Transaction-based systems include, for example, database management systems and transaction processing systems. Mechanisms supporting transaction recovery include, for example, transaction rollback and transaction journaling.

Related Controls: None.

(3) SYSTEM RECOVERY AND RECONSTITUTION | COMPENSATING SECURITY CONTROLS

[Withdrawn: Addressed through tailoring procedures].

(4) SYSTEM RECOVERY AND RECONSTITUTION | RESTORE WITHIN TIME-PERIOD

Provide the capability to restore system components within [*Assignment: organization-defined restoration time-periods*] from configuration-controlled and integrity-protected information representing a known, operational state for the components.

Supplemental Guidance: Restoration of system components includes, for example, reimaging which restores components to known, operational states.

Related Controls: CM-2, CM-6.

(5) SYSTEM RECOVERY AND RECONSTITUTION | FAILOVER CAPABILITY

[Withdrawn: Incorporated into SI-13].

(6) SYSTEM RECOVERY AND RECONSTITUTION | COMPONENT PROTECTION

Protect system components used for backup and restoration.

Supplemental Guidance: Protection of system backup and restoration components (hardware, firmware, and software) includes both physical and technical safeguards. Backup and restoration software includes, for example, router tables, compilers, and other security-relevant system software.

Related Controls: AC-3, AC-6, MP-2, MP-4, PE-3, PE-6.

References: NIST Special Publication 800-34.

CP-11 ALTERNATE COMMUNICATIONS PROTOCOLS

Control: Provide the capability to employ [*Assignment: organization-defined alternative communications protocols*] in support of maintaining continuity of operations.

Supplemental Guidance: Contingency plans and the training/testing associated with those plans, incorporate an alternate communications protocol capability as part of establishing resilience in organizational systems. Alternate communications protocols include, for example, switching from TCP/IP Version 4 to TCP/IP Version 6. Switching communications protocols may affect software applications and ~~therefore,~~operational aspects of systems. Organizations assess the potential side effects of introducing such alternate communications protocols ~~are analyzed~~ prior to implementation.

Related Controls: CP-2, CP-8, CP-13.

Control Enhancements: None.

References: None.

CP-12 SAFE MODE

Control: When [*Assignment: organization-defined conditions*] are detected, enter a safe mode of operation with [*Assignment: organization-defined restrictions of safe mode of operation*].

Supplemental Guidance: For systems supporting critical missions and business functions including, for example, military operations and weapons systems, civilian space operations, nuclear power plant operations, and air traffic control operations (especially real-time operational environments), organizations can identify certain conditions under which those systems revert to a predefined safe mode of operation. The safe mode of operation, which can be activated automatically or manually, restricts the activities or operations systems can execute when those conditions are encountered. Restriction includes, for example, allowing only certain functions that can be carried out under limited power or with reduced communications bandwidth.

Related Controls: CM-2, SC-24, SI-13, SI-17.

Control Enhancements: None.

References: None.

CP-13 ALTERNATIVE SECURITY MECHANISMS

Control: Employ [*Assignment: organization-defined alternative or supplemental security mechanisms*] for satisfying [*Assignment: organization-defined security functions*] when the primary means of implementing the security function is unavailable or compromised.

Supplemental Guidance: This control supports system resiliency, contingency planning, and continuity of operations. To ensure mission and business continuity, organizations can implement alternative or supplemental security mechanisms. These mechanisms may be less effective than the primary mechanisms ~~(e.g., not as easy to use, not as scalable, or not as secure).~~ However, having the capability to readily employ these alternative or supplemental mechanisms, enhances ~~overall~~ mission and business continuity that might otherwise be adversely impacted if operations had to be curtailed until the primary means of implementing the functions was restored. Given the cost and level of effort required to provide such alternative capabilities, this control is typically applied only to critical security capabilities provided by systems, system components, or system services. For example, an organization may issue to senior executives and system administrators one-time pads ~~in case~~if multifactor tokens, the ~~organization's~~ standard means for secure remote authentication, is compromised.

Related Controls: CP-2 CP-11, SI-13.

Control Enhancements: None.

References: None.

3.7 IDENTIFICATION AND AUTHENTICATION

Quick link to Identification and Authentication summary table

IA-1 IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES

Control:

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

1. An 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 senior management official*] to manage the identification and authentication policy and procedures;

~~b.~~c. Review and update the current identification and authentication:

1. Policy [*Assignment: organization-defined frequency*]; and

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

d. Ensure that the identification and authentication procedures implement the identification and authentication policy and controls; and

e. Develop, document, and implement remediation actions for violations of the identification and authentication policy.

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of ~~selected security~~ the controls and control enhancements in the IA family. The risk management strategy is an important factor in establishing policy and procedures ~~reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards,~~. Comprehensive policy and ~~guidance~~procedures help provide security and privacy assurance. Security and privacy program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general ~~information~~ security and privacy policy ~~for organizations or conversely,~~or can be represented by multiple policies reflecting the complex nature of ~~certain~~ organizations. The procedures can be established for ~~the~~ security ~~program in general~~and privacy programs and for ~~particular information~~ systems, if needed. ~~The~~Procedures describe how policies or controls are implemented and can be directed at the personnel 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. It is important to recognize that restating controls does not constitute an organizational ~~risk management strategy is a key factor in establishing~~ policy ~~and procedures~~or procedure.

Related Controls: AC-1, PM-9, PS-8, SI-12.

Control Enhancements: None.

References: FIPS Publication 201; NIST Special Publications 800-12, 800-30, 800-39, 800-63, 800-73, 800-76, 800-78, 800-100; NIST Interagency Report 7874.

IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

Control: Uniquely identify and authenticate organizational users or processes acting on behalf of organizational users.

Supplemental Guidance: Organizations can satisfy the identification and authentication requirements in this control by complying with the requirements in Homeland Security Presidential Directive 12. Organizational users include employees or individuals that organizations consider having the equivalent status of employees including, for example, contractors and guest researchers. This control applies to all accesses other than accesses that are explicitly identified ~~and documented~~ in AC-14 and that occur through the authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts ~~(e.g., shared privilege accounts)~~ or for detailed accountability of individual activity. Organizations employ passwords, ~~tokens~~physical authenticators, or biometrics to authenticate user identities, or in the case of multifactor authentication, some combination thereof. Access to organizational systems is defined as either local access or network access. Local access is any access to organizational systems by users or processes acting on behalf of users, where such 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 such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks ~~(e.g., the Internet).~~ Internal networks include local area networks and wide area networks. 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.

Related Controls: 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.

Control Enhancements:

(1) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | MULTIFACTOR AUTHENTICATION ~~NETWORK ACCESS~~ TO PRIVILEGED ACCOUNTS

Implement multifactor authentication for ~~network~~ access to privileged accounts.

Supplemental Guidance: Multifactor authentication requires the use of two or more different factors to achieve authentication. Factors are defined as follows: something you know, for example, a password or personal identification number (PIN); something you have, for example, a physical authenticator or cryptographic identification device~~, token);~~; or something you are, for example, a biometric. Multifactor solutions that ~~require devices separate from information systems gaining access~~feature physical authenticators include, for example, hardware ~~tokens~~authenticators providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card or the DoD common access card. In addition to ~~identifying and~~ authenticating users at the system level (i.e., at logon), organizations may also employ ~~identification and~~ authentication mechanisms at the application level, ~~when necessary~~at their discretion, to provide increased information security. ~~Identification and~~Regardless of the type of access (i.e., local, network, or remote) privileged accounts are always authenticated using multifactor options appropriate for the level of risk. Organizations can add additional security measures, such as additional or more rigorous authentication ~~requirements for other than organizational users are described in IA-8.~~ mechanisms, for specific types of access.

Related Controls: AC-5, AC-6.

~~(1)~~(2) IDENTIFICATION AND AUTHENTICATION ~~| NETWORK ACCESS TO~~ (ORGANIZATIONAL USERS) | MULTIFACTOR AUTHENTICATION TO NON-PRIVILEGED ACCOUNTS

Implement multifactor authentication for ~~network~~ access to non-privileged accounts.

Supplemental Guidance: Multifactor authentication requires the use of two or more different factors to achieve authentication. Factors are defined as follows: something you know, for

example, a personal identification number (PIN); something you have, for example, a physical authenticator or cryptographic private key stored in hardware or software; or something you are, for example, a biometric. Multifactor solutions that feature physical authenticators include, for example, hardware authenticators providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card or the DoD common access card. In addition to authenticating users at the system level, organizations may also employ authentication mechanisms at the application level, at their discretion, to provide increased information security. Organizations can also provide additional security measures, such as additional or more rigorous authentication mechanisms, for specific types of access.

Related Controls: AC-5.

(3) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | LOCAL ACCESS TO PRIVILEGED ACCOUNTS

[Withdrawn: Incorporated into IA-2(1)(2)].

~~**The information system implements multifactor authentication for local access to privileged accounts.**~~

~~**(2)**~~**(4)** IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | LOCAL ACCESS TO NON-PRIVILEGED ACCOUNTS

[Withdrawn: Incorporated into IA-2(1)(2)].

~~**The information system implements multifactor authentication for local access to non-privileged accounts.**~~

(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.

~~**The organization requires individuals to be authenticated with an individual authenticator when a group authenticator is employed.**~~

Supplemental Guidance: ~~Requiring individuals~~ Individual authentication prior to ~~use individual authenticators as a second level of~~the shared group authentication helps organizations to mitigate the risk of using group accounts or authenticators.

Related Controls: None.

~~**(3)**~~**(6)** IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO PRIVILEGED ACCOUNTS — SEPARATE DEVICE

~~**(4)** [Withdrawn: Incorporated into IA-2(1)(2)]. **The information system implements multifactor authentication for network access to privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [*Assignment: organization-defined strength of mechanism requirements*].**~~

~~**(5)**~~**(7)** IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS — SEPARATE DEVICE

[Withdrawn: Incorporated into IA-2(1)(2)

~~**The information system implements multifactor authentication for network access to non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [*Assignment: organization-defined strength of mechanism requirements*].**~~

~~**(6)**~~**(8)** ~~*IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO PRIVILEGED*~~ IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO ACCOUNTS — REPLAY RESISTANT

Implement replay-resistant authentication mechanisms for ~~network~~ access to [*Selection (one or more): privileged accounts; non-privileged accounts*].

Supplemental Guidance: Authentication processes resist replay attacks if it is impractical to achieve successful authentications by replaying previous authentication messages. Replay-resistant techniques include, for example, protocols that use nonces or challenges such as

~~Transport Layer Security (TLS) and~~ time synchronous or challenge-response one-time authenticators.

Related Controls: None.

~~(7)~~(9) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS — REPLAY RESISTANT

~~**The information system implements replay-resistant authentication mechanisms for network access to non-privileged accounts.**~~

~~Supplemental Guidance: Authentication processes resist replay attacks if it is impractical to achieve successful authentications by recording/replaying previous authentication messages. Replay-resistant techniques include, for example, protocols that use nonces or challenges such as Transport Layer Security (TLS) and time synchronous or challenge-response one-time authenticators.~~

[Withdrawn: Incorporated into IA-2(8)].

~~(8)~~(10) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | SINGLE SIGN-ON

Provide a single sign-on capability for [*Assignment: organization-defined ~~list of information system accounts and services~~*].

Supplemental Guidance: Single sign-on enables users to log in once and gain access to multiple ~~information~~ system resources. Organizations consider the operational efficiencies provided by single sign-on capabilities with the ~~increased risk from disclosures of single authenticators providing access to multiple system resources~~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 multifactor authentication for applications that may not be able to natively support this function. This situation may occur in legacy applications or systems.

Related Controls: None.

~~(9)~~(11) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | REMOTE ACCESS — SEPARATE DEVICE

~~**The information system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [*Assignment: organization-defined strength of mechanism requirements*].**~~

~~Supplemental Guidance: For remote access to privileged/non-privileged accounts, the purpose of requiring a device that is separate from the information system gaining access for one of the factors during multifactor authentication is to reduce the likelihood of compromising authentication credentials stored on the system. For example, adversaries deploying malicious code on organizational information systems can potentially compromise such credentials resident on the system and subsequently impersonate authorized users. Related control: AC-6.~~

[Withdrawn: Incorporated into IA-2(1)(2)].

~~(10)~~(12) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | ACCEPTANCE OF PIV CREDENTIALS

Accept and electronically verify Personal Identity Verification credentials.

Supplemental Guidance: This control enhancement applies to organizations implementing logical access control ~~systems (LACS)~~ and physical access control systems ~~(PACS).~~ Personal Identity Verification (PIV) credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents. ~~OMB Memorandum 11-11 requires federal agencies to continue implementing the requirements specified in HSPD-12 to enable agency-wide use of PIV credentials.~~ The adequacy and reliability of PIV card issuers are addressed and authorized using NIST Special Publication 800-79. Acceptance of PIV credentials includes derived PIV credentials, the use of which is addressed in NIST Special Publication 800-166.

Related Controls: None.

~~(11)~~(13) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | OUT-OF-BAND AUTHENTICATION

~~**The information system implements [*Assignment: organization-defined out-of-band authentication*] under [*Assignment: organization-defined conditions*].**~~

~~Supplemental Guidance: Out-of-band authentication (OOBA) refers to the use of two separate communication paths to identify and authenticate users or devices to an information system. The first path (i.e., the in-band path), is used to identify and authenticate users or devices, and generally is the path through which information flows. The second path (i.e., the out-of-band path) is used to independently verify the authentication and/or requested action. For example, a user authenticates via a notebook computer to a remote server to which the user desires access, and requests some action of the server via that communication path. Subsequently, the server contacts the user via the user's cell phone to verify that the requested action originated from the user. The user may either confirm the intended action to an individual on the telephone or provide an authentication code via the telephone. This type of authentication can be employed by organizations to mitigate actual or suspected man-in-the-middle attacks. The conditions for activation can include, for example, suspicious activities, new threat indicators or elevated threat levels, or the impact level or classification level of information in requested transactions. Related controls: IA-10, IA-11, SC-37.~~

~~References: HSPD-12; OMB Memoranda 04-04, 06-16, 11-11; FIPS Publication 201; NIST Special Publications 800-63, 800-73, 800-76, 800-78; FICAM Roadmap and Implementation Guidance; Web: http://idmanagement.gov.~~

[Withdrawn: Incorporated into IA-2(1)(2)].

References: FIPS Publications 140-2, 201, 202; NIST Special Publications 800-63, 800-73, 800-76, 800-78, 800-79, 800-156, 800-166; NIST Interagency Reports 7539, 7676, 7817, 7849, 7870, 7874, 7966.

IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION

Control: Uniquely identify and authenticate [*Assignment: organization-defined specific and/or types of devices*] before establishing a [*Selection (one or more): local; remote; network*] connection.

Supplemental Guidance: ~~Organizational~~ Devices requiring unique device-to-device identification and authentication ~~may be~~are defined by type, by device, or by a combination of type and device. ~~Information systems typically use either~~Organization-defined device types may include devices that are not owned by the organization. Systems use shared known information (e.g., Media Access Control [MAC] or Transmission Control Protocol/Internet Protocol [TCP/IP] addresses) for device identification or organizational authentication solutions (e.g., IEEE 802.1x and Extensible Authentication Protocol [EAP], RADIUS server with EAP-Transport Layer Security [TLS] authentication, Kerberos) to identify and authenticate devices on local and wide area networks. Organizations determine the required strength of authentication mechanisms ~~by~~based on the security categories of systems and mission/business requirements. Because of the challenges of implementing this control on large scale, organizations ~~are encouraged to only apply~~can restrict the application of the control to ~~those~~a limited number (and type) of devices ~~that truly~~based on organizational need ~~to support this capability.~~.

Related Controls: AC-17, AC-18, AC-19, AU-6, CA-3, CA-9, IA-4, IA-5, IA-9, IA-11, SI-4.

Control Enhancements:

(1) DEVICE IDENTIFICATION AND AUTHENTICATION | CRYPTOGRAPHIC BIDIRECTIONAL AUTHENTICATION

Authenticate [*Assignment: organization-defined specific devices and/or types of devices*] before establishing [*Selection (one or more): local; remote; network*] connection using bidirectional authentication that is cryptographically based.

Supplemental Guidance: A local connection is any connection with a device communicating without the use of a network. A network connection is any connection with a device that communicates through a network ~~(e.g., local area or wide area network, Internet).~~ A remote connection is any connection with a device communicating through an external network ~~(e.g.,~~

~~the Internet).~~. Bidirectional authentication provides stronger safeguards to validate the identity of other devices for connections that are of greater risk ~~(e.g., remote connections).~~ .

Related Controls: SC-8, SC-12, SC-13.

(2) DEVICE IDENTIFICATION AND AUTHENTICATION | CRYPTOGRAPHIC BIDIRECTIONAL NETWORK AUTHENTICATION

[Withdrawn: Incorporated into IA-3(1)].

(3) DEVICE IDENTIFICATION AND AUTHENTICATION | DYNAMIC ADDRESS ALLOCATION

(a) ~~Standardizes~~**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.**

Supplemental Guidance: DHCP and DHCPv6 are typical protocols that enable clients ~~obtaining~~ to dynamically obtain Internet Protocol address leases ~~for IP addresses~~ from DHCP servers~~, is a typical example of dynamic address allocation for devices.~~ .

Related Controls: None.

(4) DEVICE IDENTIFICATION AND AUTHENTICATION | DEVICE ATTESTATION

Handle device identification and authentication based on attestation by [*Assignment: organization-defined configuration management process*].

Supplemental Guidance: Device attestation refers to the identification and authentication of a device based on its configuration and known operating state. This might be determined via some cryptographic hash of the device. If device attestation is the means of identification and authentication, then it is important that patches and updates to the device are handled via a configuration management process such that the patches and updates are done securely and at the same time do not disrupt the identification and authentication to other devices.

Related Controls: CM-2, CM-3, CM-6.

References: None.

IA-4 IDENTIFIER MANAGEMENT

Control: Manage system identifiers by:

a. Receiving authorization from [*Assignment: organization-defined personnel or roles*] to assign an individual, group, role, or device identifier;

b. Selecting an identifier that identifies an individual, group, role, or device;

c. Assigning the identifier to the intended individual, group, role, or device; and

d. Preventing reuse of identifiers for [*Assignment: organization-defined time-period*].

~~**(1)** Disabling the identifier after [*Assignment: organization-defined time period of inactivity*].~~

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

Related Controls: IA-2, IA-3, IA-5, IA-8, IA-9, MA-4, PE-2, PE-3, PE-4, PL-4, PM-12, PS-3, PS-4, PS-5, SC-37.

Control Enhancements:

(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 electronic mail accounts.

Supplemental Guidance: Prohibiting the use of systems account identifiers that are the same as some public identifier such as the individual identifier section of an electronic mail address, makes it more difficult for adversaries to guess user identifiers on organizational systems. The use of this control alone only complicates guessing of identifiers and must be combined with appropriate protections for authenticators and attributes to protect the account as a whole.

Related Controls: AT-2.

(2) IDENTIFIER MANAGEMENT | SUPERVISOR AUTHORIZATION

~~**The organization requires that the registration process to receive an individual identifier includes supervisor authorization.**~~

[Withdrawn: Incorporated into IA-12(1)].

(3) IDENTIFIER MANAGEMENT | MULTIPLE FORMS OF CERTIFICATION

~~**The organization requires multiple forms of certification of individual identification such as documentary evidence or a combination of documents and biometrics be presented to the registration authority.**~~

~~Supplemental Guidance: Requiring multiple forms of identification reduces the likelihood of individuals using fraudulent identification to establish an identity, or at least increases the work factor of potential adversaries.~~

[Withdrawn: Incorporated into IA-12(2)].

(4) IDENTIFIER MANAGEMENT | IDENTIFY USER STATUS

Manage individual identifiers by uniquely identifying each individual as [*Assignment: organization-defined characteristic identifying individual status*].

Supplemental Guidance: Characteristics identifying the status of individuals include, for example, contractors and foreign nationals. Identifying the status of individuals by specific 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.

Related Controls: None.

(5) IDENTIFIER MANAGEMENT | DYNAMIC MANAGEMENT

Manage individual identifiers dynamically.

Supplemental Guidance: In contrast to conventional approaches to identification which presume static accounts for preregistered users, many distributed ~~systems including, for example, service-oriented architectures, rely on establishing~~systems establish identifiers at run time for entities that were previously unknown. In these situations, organizations anticipate and provision for the dynamic establishment of identifiers. Pre-established trust relationships and mechanisms with appropriate authorities to validate identities and related credentials are essential.

Related Controls: AC-16.

(6) IDENTIFIER MANAGEMENT | CROSS-ORGANIZATION MANAGEMENT

Coordinate with [*Assignment: organization-defined external organizations*] for cross-organization management of identifiers.

Supplemental Guidance: Cross-organization identifier management provides the capability for organizations to appropriately identify individuals, groups, roles, or devices when conducting cross-organization activities involving the processing, storage, or transmission of information.

Related Controls: AU-16, IA-2, IA-5.

(7) IDENTIFIER MANAGEMENT | IN-PERSON REGISTRATION

~~**The organization requires that the registration process to receive an individual identifier be conducted in person before a designated registration authority.**~~

Supplemental Guidance: ~~In person registration reduces the likelihood of fraudulent identifiers being issued because it requires the physical presence of individuals and actual face-to-face interactions with designated registration authorities.~~

[Withdrawn: Incorporated into IA-12(4)].

(8) IDENTIFIER MANAGEMENT | PAIRWISE PSEUDONYMOUS IDENTIFIERS

Generate pairwise pseudonymous identifiers.

Supplemental Guidance: Generating distinct pairwise pseudonymous identifiers, with no identifying information about a subscriber, discourages subscriber activity tracking and profiling beyond the operational requirements established by an organization. The pairwise pseudonymous identifiers are unique to each relying party, except in situations where relying parties show a demonstrable relationship justifying an operational need for correlation, or all parties consent to being correlated in such a manner.

Related Controls: IA-5.

References: FIPS Publication 201; NIST Special Publications 800-63, 800-73, 800-76, 800-78.

IA-5 AUTHENTICATOR MANAGEMENT

Control: Manage system authenticators by:

a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;

b. Establishing initial authenticator content for any authenticators ~~defined~~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/compromised or damaged authenticators, and for revoking authenticators;

~~e. Changing default content of authenticators prior to information system installation;~~

~~f.~~e. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;

~~g.~~f. Changing/refreshing authenticators [*Assignment: organization-defined time~~-~~period by authenticator type*];

~~h.~~g. Protecting authenticator content from unauthorized disclosure and modification;

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

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

Supplemental Guidance: Examples of individual authenticators include passwords, ~~tokens, biometrics, PKI certificates~~cryptographic devices, one-time password devices, and key cards. The initial authenticator content is the actual content ~~(e.g.,~~of the authenticator, for example, the initial password~~) as opposed to~~. In contrast, the requirements about authenticator content ~~(e.g.,~~include, for example, the minimum password length. Developers may ship system components with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant security risk. The requirement to protect individual authenticators may be implemented via control PL-4 or PS-6 for authenticators in the possession of individuals and by controls AC-3, AC-6, and SC-28 for authenticators stored in organizational systems including, for example, passwords stored in hashed or encrypted formats or files containing encrypted or hashed passwords accessible with administrator privileges. Systems support ~~individual~~ authenticator management by organization-defined settings and restrictions for various authenticator characteristics including, for example, minimum password length, ~~password composition,~~ validation time window for time synchronous one-time tokens, and number of allowed rejections during the verification stage of

biometric authentication. Actions that can be taken to safeguard individual authenticators include, for example, maintaining possession of authenticators, not loaning or sharing authenticators with others, and reporting lost, stolen, or compromised authenticators immediately. Authenticator management includes issuing and revoking, when no longer needed, authenticators for temporary access such as that required for remote maintenance. Device authenticators include, for example, certificates and passwords.

Related Controls: AC-3, AC-6, CM-6, IA-2, IA-4, IA-7, IA-8, IA-9, MA-4, PE-2, PL-4.

Control Enhancements:

(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 have been compromised;

(b) Verify, when users create or update passwords, that the passwords are not found on the organization-defined list of commonly-used, expected, or compromised passwords;

(c) Transmit only cryptographically-protected passwords;

(d) Store passwords using an approved hash algorithm and salt, preferably using a keyed hash;

(e) Require immediate selection of a new password upon account recovery; and

(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.

Supplemental Guidance: This control enhancement applies to passwords regardless of whether they are used in single-factor or multi-factor authentication. Long passwords or passphrases are preferable over shorter passwords. Enforced composition rules provide marginal security benefit while decreasing usability. Account recovery can occur, for example, in situations when a password is forgotten. Cryptographically-protected passwords include, for example, salted one-way cryptographic hashes of passwords. The list of commonly-used, expected, or compromised passwords may include, for example, passwords obtained from previous breach corpuses, dictionary words, and repetitive or sequential characters. Examples include aaaaaaa, 1234abcd, and qwertyuiop. The list can also include context specific words, for example, the name of the service, username, and derivatives thereof.

~~**(a) Enforces minimum password complexity of [*Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type*];**~~

~~**(b) Enforces at least the following number of changed characters when new passwords are created: [*Assignment: organization-defined number*];**~~

~~**(c) Enforces password minimum and maximum lifetime restrictions of [*Assignment: organization-defined numbers for lifetime minimum, lifetime maximum*];**~~

~~**(d) Prohibits password reuse for [*Assignment: organization-defined number*] generations; and**~~

~~**(e) Allows the use of a temporary password for system logons with an immediate change to a permanent password.**~~

Supplemental Guidance: This control enhancement applies to passwords regardless of whether they are used in single-factor or multi-factor authentication~~ of individuals using passwords as individual or group authenticators, and in a similar manner, when passwords are part of multifactor authenticators. This control enhancement does *not* apply when passwords are used to unlock hardware authenticators (e.g., Personal Identity Verification cards). The implementation of such password mechanisms may not meet all of the requirements in the enhancement.~~. Long passwords or passphrases are preferable over shorter passwords. Enforced composition rules provide marginal security benefit while decreasing usability. Account recovery can occur, for example, in situations when a password is forgotten. Cryptographically-protected passwords include, for example, ~~encrypted versions of passwords and~~salted one-way cryptographic hashes of passwords. ~~The number of changed characters refers to the number of changes required with respect to the total number of positions in the~~

~~current password. Password lifetime restrictions do not apply to temporary passwords. To mitigate certain brute-force attacks against passwords, organizations may also consider salting passwords.~~ The list of commonly-used, expected, or compromised passwords may include, for example, passwords obtained from previous breach corpuses, dictionary words, and repetitive or sequential characters. Examples include aaaaaaa, 1234abcd, and qwertyuiop. The list can also include context specific words, for example, the name of the service, username, and derivatives thereof.

Related Controls: IA-6.

(2) AUTHENTICATOR MANAGEMENT | ~~*PKI*~~PUBLIC KEY-BASED AUTHENTICATION

~~for PKI~~For public key-based authentication:

(a) ~~Validates certifications~~Enforce authorized access to the corresponding private key; and

(b) Map the authenticated identity to the account of the individual or group; and

When public key infrastructure (PKI) is used:

~~(a)~~(c) Validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information; and

~~(b)~~(d) Implement a local cache of revocation data to support path discovery and validation ~~in case of inability to access revocation information via the network~~.

Supplemental Guidance: Public key cryptography is a valid authentication mechanism for individuals and machines/devices. When PKI is leveraged, status information for certification paths includes, for example, certificate revocation lists or certificate status protocol responses. For PIV cards, the validation of ~~certifications~~certificates involves the construction and verification of a certification path to the Common Policy Root trust anchor ~~including certificate policy processing. Related control: IA-6.~~which includes certificate policy processing. Implementing a local cache of revocation data to support path discovery and validation supports system availability in situations where organizations are unable to access revocation information via the network

Related Controls: IA-3, SC-17.

(3) AUTHENTICATOR MANAGEMENT | IN-PERSON OR TRUSTED ~~*THIRD-*~~EXTERNAL PARTY REGISTRATION

~~**The organization requires that the registration process to receive [*Assignment: organization-defined types of and/or specific authenticators*] be conducted [*Selection: in person; by a trusted third party*] before [*Assignment: organization-defined registration authority*] with authorization by [*Assignment: organization-defined personnel or roles*].**~~

[Withdrawn: Incorporated into IA-12(4)].

(4) AUTHENTICATOR MANAGEMENT | AUTOMATED SUPPORT ~~-~~FOR PASSWORD STRENGTH DETERMINATION

~~**The organization employs automated tools to determine if password authenticators are sufficiently strong to satisfy [*Assignment: organization-defined requirements*].**~~

~~Supplemental Guidance: This control enhancement focuses on the creation of strong passwords and the characteristics of such passwords (e.g., complexity) prior to use, the enforcement of which is carried out by organizational information systems in IA-5 (1). Related controls: CA-2, CA-7, RA-5.~~

[Withdrawn: Incorporated into IA-5(1)].

(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.

Supplemental Guidance: This control enhancement 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 the 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.

Related Controls: None.

(6) AUTHENTICATOR MANAGEMENT | PROTECTION OF AUTHENTICATORS

Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access.

Supplemental Guidance: For systems containing multiple security categories of information without reliable physical or logical separation between categories, authenticators used to grant access to the systems are protected commensurate with the highest security category of information on the systems. Security categories of information are determined as part of the security categorization process.

Related Controls: RA-2.

(7) AUTHENTICATOR MANAGEMENT | NO EMBEDDED UNENCRYPTED STATIC AUTHENTICATORS

Ensure that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.

Supplemental Guidance: Organizations exercise caution in 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. This is irrespective of whether that representation is perhaps an encrypted version of something else ~~(e.g., a password).~~.

Related Controls: None.

(8) AUTHENTICATOR MANAGEMENT | MULTIPLE SYSTEM ACCOUNTS

Implement [*Assignment: organization-defined security safeguards*] to manage the risk of compromise due to individuals having accounts on multiple systems.

Supplemental Guidance: When individuals have accounts on multiple systems, there is the risk that a compromise of one account may lead to the compromise of other accounts if individuals use the same authenticators. Possible alternatives include: having different authenticators on all systems; employing some form of single sign-on mechanism; or using some form of one-time passwords on all systems.

Related Controls: None.

(9) AUTHENTICATOR MANAGEMENT | ~~*CROSS-ORGANIZATION*~~FEDERATED CREDENTIAL MANAGEMENT

~~**The organization coordinates with**~~**Use [*Assignment: organization-defined external organizations*] ~~for cross-organization management of credentials~~to federate authenticators.**

Supplemental Guidance: ~~Cross-organization management of credentials~~Federation provides the capability for organizations to appropriately authenticate individuals~~, groups, roles, or~~ and devices when conducting cross-organization activities involving the processing, storage, or transmission of information.

Related Controls: AU-7, AU-16.

(10) AUTHENTICATOR MANAGEMENT | DYNAMIC CREDENTIAL ~~*ASSOCIATION*~~BINDING

~~**The information system**~~**Bind identities and authenticators dynamically ~~provisions identities~~.**

Supplemental Guidance: Authentication requires some form of binding between an identity and the authenticator used to confirm the identity. In conventional approaches, this binding is established by pre-provisioning both the identity and the authenticator to the system. For example, the binding between a username (i.e., identity) and a password (i.e., authenticator) is accomplished by provisioning the identity and authenticator as a pair in the system. New authentication techniques allow the binding between the identity and the authenticator to be implemented outside a system. For example, with smartcard credentials, the identity and the authenticator are bound together on the smartcard. Using these credentials, systems can authenticate identities that have not been pre-provisioned, dynamically provisioning the identity after authentication. In these situations, organizations can anticipate the dynamic provisioning of identities. Pre-established trust relationships and mechanisms with appropriate authorities to validate identities and related credentials are essential.

Related Controls: AU-16, IA-5.

(11) AUTHENTICATOR MANAGEMENT | HARDWARE TOKEN-BASED AUTHENTICATION

~~**The information system, for hardware token-based authentication, employs mechanisms that satisfy [*Assignment: organization-defined token quality requirements*].**~~

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

[Withdrawn: Incorporated into IA-2(1)(2)].

(12) AUTHENTICATOR MANAGEMENT | BIOMETRIC AUTHENTICATION PERFORMANCE

For biometric-based authentication, employ mechanisms that satisfy [*Assignment: organization-defined biometric quality requirements*].

Supplemental Guidance: Unlike password-based authentication which provides exact matches of user-input passwords to stored passwords, biometric authentication does not provide such exact matches. Depending upon the type of biometric and the type of collection mechanism, there is likely to be some divergence from the presented biometric and stored biometric which serves as the basis of comparison. ~~There will likely be both false positives and false negatives when making such comparisons.~~ The matching performance is the rate at which ~~the false accept and false reject rates are equal is known as the crossover rate.~~a biometric algorithm correctly results in a match for a genuine user and rejects other users. Biometric ~~quality~~performance requirements include, for example, ~~acceptable crossover rates, as that essentially~~the match rate as this reflects the accuracy of the biometric matching algorithm being used by a system.

Related Controls: AC-7.

(13) AUTHENTICATOR MANAGEMENT | EXPIRATION OF CACHED AUTHENTICATORS

Prohibit the use of cached authenticators after [*Assignment: organization-defined time-period*].

Supplemental Guidance: None.

Related Controls: None.

(14) AUTHENTICATOR MANAGEMENT | MANAGING CONTENT OF PKI TRUST STORES

For PKI-based authentication, employ a deliberate organization-wide methodology for managing the content of PKI trust stores installed across all platforms including networks, operating systems, browsers, and applications.

Supplemental Guidance: None.

Related Controls: None.

(15) AUTHENTICATOR MANAGEMENT | ~~*FICAM*~~GSA-APPROVED PRODUCTS AND SERVICES

Use only ~~FICAM~~General Services Administration-approved ~~path discovery~~ and ~~validation~~validated products and services.

Supplemental Guidance: ~~Federal Identity, Credential, and Access Management (FICAM~~General Services Administration (GSA)-approved ~~path discovery and validation~~ products and services are ~~those~~the products and services that have been approved through the ~~FICAM~~GSA conformance program, where applicable, and posted to the GSA Approved Products List.

Related Controls: None.

(16) AUTHENTICATOR MANAGEMENT | IN-PERSON OR TRUSTED EXTERNAL PARTY AUTHENTICATOR ISSUANCE

Require that the issuance of [*Assignment: organization-defined types of and/or specific authenticators*] be conducted [*Selection: in person; by a trusted external party*] before [*Assignment: organization-defined registration authority*] with authorization by [*Assignment: organization-defined personnel or roles*].

Supplemental Guidance: None.

Related Controls: IA-12.

(17) AUTHENTICATOR MANAGEMENT | PRESENTATION ATTACK DETECTION FOR BIOMETRIC AUTHENTICATORS

Employ presentation attack detection mechanisms for biometric-based authentication.

Supplemental Guidance: Biometric characteristics do not constitute secrets. Such characteristics can be obtained by online web accesses; taking a picture of someone with a camera phone to obtain facial images with or without their knowledge; lifting from objects that someone has

touched, for example, a latent fingerprint; or capturing a high-resolution image, for example, an iris pattern. Presentation attack detection technologies including, for example, liveness detection, can mitigate the risk of these types of attacks by making it more difficult to produce artifacts intended to defeat the biometric sensor.

Related Controls: AC-7.

References: FIPS Publications 140-2, 180-4, 201, 202; NIST Special Publications 800-73, 800-63, 800-76, 800-78; NIST Interagency Reports 7539, 7817, 7849, 7870, 8040.

IA-6 AUTHENTICATOR FEEDBACK

Control: Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.

Supplemental Guidance: The feedback from systems does not provide information that would allow unauthorized individuals to compromise authentication mechanisms. For some types of systems or system components, for example, desktops/notebooks with relatively large monitors, the threat (referred to as shoulder surfing) may be significant. For other types of systems or components, for example, mobile devices with ~~2-4 inch screens~~small displays, this threat may be less significant, and ~~may need to be~~is balanced against the increased likelihood of typographic input errors due to the small keyboards. Therefore, the means for obscuring authenticator feedback is selected accordingly. Obscuring authenticator feedback ~~of authentication information~~ includes, for example, displaying asterisks when users type passwords into input devices, or displaying feedback for a very limited time before fully obscuring it.

Related Controls: AC-3.

Control Enhancements: None.

References: None.

IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION

Control: Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable ~~federal~~ laws, Executive Orders, directives, policies, regulations, standards, and guidelines for such authentication.

Supplemental Guidance: Authentication mechanisms may be required within a cryptographic module to authenticate an operator accessing the module and to verify that the operator is authorized to assume the requested role and perform services within that role.

Related Controls: AC-3, IA-5, SA-4, SC-12, SC-13.

Control Enhancements: None.

References: FIPS Publication 140-2.

IA-8 IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)

Control: Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.

Supplemental Guidance: Non-organizational users include system users other than organizational users explicitly covered by IA-2. These individuals are uniquely identified and authenticated for accesses other than those accesses explicitly identified and documented in AC-14. ~~In accordance with the E-Authentication E-Government initiative,~~Identification and authentication of non-organizational users accessing federal ~~information~~ systems may be required to protect federal, proprietary, or privacy-related information (with exceptions noted for national security systems). Organizations ~~use risk assessments to determine authentication needs and~~ consider many factors including scalability, practicality, security, and privacy in balancing the need to ensure ease of use for access to federal information and systems with the need to protect and adequately mitigate risk

~~IA-2 addresses identification and authentication requirements for access to information systems by organizational users~~.

Related Controls: 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, SA-12, SC-8.

Control Enhancements:

(1) IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | ACCEPTANCE OF PIV CREDENTIALS FROM OTHER AGENCIES

Accept and electronically verify Personal Identity Verification credentials from other federal agencies.

Supplemental Guidance: This control enhancement applies to both logical and physical access control systems. Personal Identity Verification (PIV) credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting ~~guidance documents. OMB Memorandum 11-11 requires federal agencies to continue implementing the requirements specified in HSPD-12 to enable agency-wide use~~guidelines. The adequacy and reliability of PIV ~~credentials.~~ card issuers are addressed and authorized using NIST Special Publication 800-79.

Related Controls: PE-3.

(2) IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | ACCEPTANCE OF ~~*THIRD-PARTY*~~EXTERNAL CREDENTIALS

Accept only external credentials that are NIST compliant.

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

Supplemental Guidance: This control enhancement ~~typically~~ applies to organizational systems that are accessible to the public, for example, public-facing websites. ~~Third-party~~External credentials are those credentials issued by nonfederal government entities ~~approved by the Federal Identity, Credential, and Access Management (FICAM) Trust Framework Solutions initiative.~~. Such credentials are certified as compliant with NIST Special Publication 800-63 by an approved accreditation authority. Approved ~~third-party~~external credentials meet or exceed the set of minimum federal government-wide technical, security, privacy, and organizational maturity requirements. This allows federal government relying parties to trust such credentials at their approved assurance levels.

Related Controls: None.

~~**(2)**~~**(3)** IDENTIFICATION AND IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | USE OF FICAM-APPROVED PRODUCTS

~~**The organization employs only FICAM-approved information system components in [*Assignment: organization-defined information systems*] to accept third-party credentials.**~~

~~Supplemental Guidance: This control enhancement typically applies to information systems that are accessible to the general public, for example, public-facing websites. FICAM-approved information system components include, for example, information technology products and software libraries that have been approved by the Federal Identity, Credential, and Access Management conformance program. Related control: SA-4.~~

[Withdrawn: Incorporated into IA-8(2)].

~~**(3)**~~**(4)** IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | USE OF ~~*FICAM*~~NIST-ISSUED PROFILES

~~**The information system conforms to FICAM**~~**Conform to NIST-issued profiles for identity management.**

Supplemental Guidance: This control enhancement addresses open identity management standards. To ensure that these identity management standards are viable, robust, reliable, sustainable ~~(e.g., available in commercial information technology products),~~, and interoperable as documented, the United States Government assesses and scopes ~~identity management~~the standards and technology implementations against applicable ~~federal legislation~~laws, Executive Orders, directives, policies, ~~and requirements.~~ regulations, standards, and guidelines. The result is ~~FICAM~~NIST-issued implementation profiles of

approved protocols ~~(e.g., FICAM-approved protocols such as SAML 2.0 and OpenID 2.0, as well as other protocols such as the FICAM Backend Attribute Exchange). Related control: SA-4.~~

Related Controls: None.

~~(4)~~(5) *IDENTIFICATION AND AUTHENTICATION* (NON-ORGANIZATIONAL USERS) | ACCEPTANCE OF PIV-I CREDENTIALS

Accept and electronically verify Personal Identity Verification-I (PIV-I) credentials.

Supplemental Guidance: This control enhancement applies to both logical access control and physical access control systems. It addresses ~~Non-Federal~~Nonfederal Issuers ~~(NFIs)~~ of identity cards that desire to interoperate with United States Government Personal Identity Verification (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 ~~suitable for Assurance Level 4~~ commensurate with the PIV credentials as defined in ~~OMB Memorandum 04-04 and NIST Special Publication 800-63, and multifactor authentication as defined in NIST Special Publication 800-116.~~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 the FBCA~~ with policies that have been mapped and approved as meeting the requirements of the PIV-I policies defined in the FBCA certificate policy.

Related Controls: None.

(6) IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | DISASSOCIABILITY

Implement [*Assignment: organization-defined measures*] to disassociate user attributes or credential assertion relationships among individuals, credential service providers, and relying parties.

Supplemental Guidance: Federated identity solutions can create increased privacy risks due to tracking and profiling of individuals. Using identifier mapping tables or privacy-enhancing 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.

Related Controls: None.

References: FIPS Publication 201; NIST Special Publications 800-63, 800-79, 800-116; NIST Interagency Report 8062.

IA-9 SERVICE IDENTIFICATION AND AUTHENTICATION

Control: Identify and authenticate [*Assignment: organization-defined system services*~~]~~ ~~using [*Assignment: organization-defined security safeguards*]~~. *and applications*] before establishing communications with devices, users, or other services or applications.

Supplemental Guidance: ~~This control supports service-oriented architectures and other distributed architectural approaches requiring the identification and authentication of information system services. In such architectures, external services often appear dynamically. Therefore, information systems should be able to determine in a dynamic manner, if external providers and associated services are authentic. Safeguards implemented by organizational information systems to validate provider and service authenticity~~Services that may require identification and authentication include, for example, web applications using digital certificates or services/applications that query a database. Identification and authentication methods for system services/applications include, for example, information or code signing, provenance graphs, and/or electronic signatures indicating ~~or including~~ the sources of services.

Related Controls: IA-3, IA-4, IA-5.

Control Enhancements:

(1) SERVICE IDENTIFICATION AND AUTHENTICATION | INFORMATION EXCHANGE

Ensure that service providers receive, validate, and transmit identification and authentication information.

Supplemental Guidance: None.

Related Controls: None.

(2) SERVICE IDENTIFICATION AND AUTHENTICATION | TRANSMISSION OF DECISIONS

Transmit identification and authentication decisions between [*Assignment: organization-defined services*] consistent with organizational policies.

Supplemental Guidance: For distributed architectures ~~(e.g., service-oriented architectures),~~ the decisions regarding the validation of identification and authentication claims may be made by services separate from the services acting on those decisions. In such situations, it is necessary to provide the identification and authentication decisions (instead of the actual identifiers and authenticators) to the services that need to act on those decisions.

Related Controls: SC-8.

References: None.

IA-10 ADAPTIVE ~~IDENTIFICATION AND~~ AUTHENTICATION

Control: Require individuals accessing the system to employ [*Assignment: organization-defined supplemental authentication techniques or mechanisms*] under specific [*Assignment: organization-defined circumstances or situations*].

Supplemental Guidance: Adversaries may compromise individual authentication mechanisms and subsequently attempt to impersonate legitimate users. This situation can potentially occur with any authentication mechanisms employed by organizations. To address this threat, organizations may employ specific techniques or mechanisms and establish protocols to assess suspicious behavior ~~(e.g., individuals~~. Such behavior may include, for example, accessing information that ~~they~~individuals do not typically access as part of their ~~normal~~ duties, roles, or responsibilities~~,~~; accessing greater quantities of information than the individuals would routinely access; or attempting to access information from suspicious network addresses. In situations when pre-established conditions or triggers occur, organizations can require ~~selected~~ individuals to provide additional authentication information. Another potential use for adaptive ~~identification and~~ authentication is to increase the strength of mechanism based on the number and/or types of records being accessed. ~~Related~~ Adaptive authentication does not replace and is not used to avoid multifactor mechanisms, but can augment implementations of these controls.

Related Controls: IA-2, IA-8.

Control Enhancements: None.

References: NIST Special Publication 800-63.

IA-11 RE-AUTHENTICATION

Control: Require users~~and devices~~ to re-authenticate when [*Assignment: organization-defined circumstances or situations requiring re-authentication*].

Supplemental Guidance: In addition to the re-authentication requirements associated with ~~session~~device locks, organizations may require re-authentication of individuals ~~and/or devices~~ in ~~other~~certain situations including, for example, when authenticators ~~change; (ii), when~~ or roles change; when security categories of systems change; when the execution of privileged functions occurs; after a fixed time-period; or periodically.

Related Controls: AC-3, AC-11, IA-2, IA-3, IA-8.

Control Enhancements: None.

References: None.

IA-12 IDENTITY PROOFING

Control:

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.

Supplemental Guidance: Identity proofing is the process of collecting, validating, and verifying user's identity information for the purposes of issuing credentials for accessing a system. This control is intended to mitigate threats to the registration of users and the establishment of their accounts. Standards and guidelines specifying identity assurance levels for identity proofing include NIST Special Publications 800-63 and 800-63A.

Related Controls: IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-8.

(1) IDENTITY PROOFING | SUPERVISOR AUTHORIZATION

Require that the registration process to receive an account for logical access includes supervisor or sponsor authorization.

Supplemental Guidance: None.

Related Controls: None.

(2) IDENTITY PROOFING | IDENTITY EVIDENCE

Require evidence of individual identification be presented to the registration authority.

Supplemental Guidance: Requiring identity evidence, such as documentary evidence or a combination of documents~~, and disseminates~~ and biometrics, reduces the likelihood of individuals using fraudulent identification to establish an identity, or at least increases the work factor of potential adversaries. Acceptable forms of evidence are consistent with the risk to the systems, roles, and privileges associated with the user's account.

Related Controls: None.

(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*].

Supplemental Guidance: Validating and verifying identity evidence increases the assurance that that accounts, identifiers, and authenticators are being issued to the correct user. Validation refers to the process of confirming that the evidence is genuine and authentic and that the data contained in the evidence is correct, current, and related to an actual person or 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 risk to the systems, roles, and privileges associated with the users account

Related Controls: None.

(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.

Supplemental Guidance: 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.

Related Controls: None.

(5) IDENTITY PROOFING | ADDRESS CONFIRMATION

Require that a [*Selection: registration code; notice of proofing*] be delivered through an out-of-band channel to verify the users address (physical or digital) of record.

Supplemental Guidance: To make it more difficult for adversaries to pose as legitimate users during the identity proofing process, organizations can use out-of-band methods to increase assurance that the individual associated with an address of record was the same person that participated in the registration. Confirmation can take the form of a temporary enrollment code or a notice of proofing. The delivery address for these artifacts are obtained from records and not self-asserted by the user. The address can include a physical or a digital address. A home address is an example of a physical address. Email addresses and telephone numbers are examples of digital addresses.

Related Controls: IA-12.

(6) IDENTITY PROOFING | ACCEPT EXTERNALLY-PROOFED IDENTITIES

Accept externally-proofed identities at [*Assignment: organization-defined identity assurance level*].

Supplemental Guidance: To limit unnecessary re-proofing of identities, particularly of non-PIV users, organizations accept proofing conducted at a commensurate level of assurance by other agencies or organizations. Proofing is consistent with organizational security policy and with the identity assurance level appropriate for the system, application, or information accessed. This is a core component of managing federated identities across agencies and organizations.

Related Controls: IA-3, IA-4, IA-5, IA-8.

References: FIPS Publication 201; NIST Special Publications 800-63, 800-63A.

3.8 INDIVIDUAL PARTICIPATION

Quick link to Individual Participation summary table

IP-1 INDIVIDUAL PARTICIPATION POLICY AND PROCEDURES

Control:

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

1. An individual participation 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 individual participation policy and the associated individual participation controls;

b. Designate an [*Assignment: organization-defined senior management official*] to manage the individual participation policy and procedures;

c. Review and update the current individual participation:

1. Policy [*Assignment: organization-defined frequency*]; and

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

d. Ensure that the individual participation procedures implement the individual participation policy and controls; and

e. Develop, document, and implement remediation actions for violations of the individual participation policy.

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of the controls and control enhancements in the IP family. The risk management strategy is an important factor in establishing policy and procedures. Comprehensive policy and procedures help provide security and privacy assurance. Security and privacy program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general security and privacy policy or can be represented by multiple policies reflecting the complex nature of organizations. The procedures can be established for security and privacy programs and for systems, if needed. Procedures describe how policies or controls are implemented and can be directed at the personnel 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. It is important to recognize that restating controls does not constitute an organizational policy or procedure.

Related Controls: PM-9, PS-8, SI-12.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-30, 800-39, 800-100.

IP-2 CONSENT

Control: Implement [*Assignment: organization-defined tools or mechanisms*] for users to authorize the processing of their personally identifiable information prior to its collection that:

a. Use plain language and provide examples to illustrate the potential privacy risks of the authorization; and

b. Provide a means for users to decline the authorization.

Supplemental Guidance: This control transfers risk that arises from the processing of personally identifiable information from the organization to an individual. It is only selected as required by law or regulation or when individuals can be reasonably expected to understand and accept any privacy risks arising from their authorization. Organizations consider whether other controls may more effectively mitigate privacy risk either alone or in conjunction with consent.

To help users understand the risks being accepted when providing consent, organizations write materials in plain language and avoid technical jargon. The examples required in IP-2 a. focus on key points necessary for user decision-making. When developing or purchasing consent tools, organizations consider the application of good information design procedures in all user-facing consent materials; use of active voice and conversational style; logical sequencing of main points; consistent use of the same word (rather than synonyms) to avoid confusion; the use of bullets, numbers, and formatting where appropriate to aid readability; and legibility of text, such as font style, size, color, and contrast with surrounding background.

Related Controls: AC-16, IP-4.

Control Enhancements:

(1) CONSENT | ATTRIBUTE MANAGEMENT

Allow data subjects to tailor use permissions to selected attributes.

Supplemental Guidance: Allowing individuals to select how specific data attributes may be further used or disclosed beyond the original use may help reduce privacy risk arising from the most sensitive of the data attributes while maintaining utility of the data.

Related Controls: None.

(2) CONSENT | JUST-IN-TIME NOTICE OF CONSENT

Present authorizations to process personally identifiable information in conjunction with the data action or [*Assignment: organization-defined frequency*].

Supplemental Guidance: If the circumstances under which an individual gave consent have changed or a significant amount of time has passed since an individual gave consent for the processing of his or her personally identifiable information, the data subject's assumption about how the information is being processed might no longer be accurate or reliable. Just-in-time notice can help maintain individual satisfaction with how the personally identifiable information is being processed.

Related Controls: None.

References: NIST Special Publication 800-63; NIST Interagency Report 8062.

IP-3 REDRESS

Control:

a. Establish and implement a process for individuals to have inaccurate personally identifiable information maintained by the organization corrected or amended; and

b. Establish and implement a process for disseminating corrections or amendments of personally identifiable information to other authorized users of the personally identifiable information.

Supplemental Guidance: Redress supports the ability of individuals to ensure the accuracy of their personally identifiable information held by organizations. Effective redress processes demonstrate organizational commitment to data quality especially in those business functions where inaccurate data may result in inappropriate decisions or the denial of benefits and services to individuals. Organizations use discretion in determining if records are to be corrected or amended, based on the scope of redress requests, the changes sought, and the impact of the changes. Other authorized users of personally identifiable information include, for example, external information-sharing partners.

An effective redress process includes: providing effective notice of the existence of a personally identifiable information collection; providing plain language explanations of the processes and mechanisms for requesting access to records; establishing the criteria for submitting requests for correction or amendment of records; implementing resources to analyze and adjudicate requests; implementing means of correcting or amending data collections; and reviewing any decisions that may have been the result of inaccurate information.

Related Controls: IP-4, IP-6, IR-7, PM-28.

Control Enhancements:

(1) REDRESS | NOTICE OF CORRECTION OR AMENDMENT

Notify affected individuals if their personally identifiable information has been corrected or amended.

Supplemental Guidance: Where personally identifiable information is corrected or amended, organizations take steps to ensure that all authorized recipients of such information and the individual with which the information is associated, are informed of the corrected or amended information.

Related Controls: None.

(2) REDRESS | APPEAL

Provide [*Assignment: organization-defined process*] for individuals to appeal an adverse decision and have incorrect information amended.

Supplemental Guidance: The Senior Agency Official for Privacy ensures that practical means and mechanisms exist and are accessible for individuals to seek the correction or amendment of their personally identifiable information. Redress processes are clearly defined and publicly available. Additionally, redress processes include the provision of responses to individuals of decisions to deny requests for correction or amendment. The responses include the reasons for the decisions, a means to record individual objections to the decisions, and finally, a means of requesting reviews of the initial determinations.

Related Controls: None.

References: None.

IP-4 PRIVACY NOTICE

Control:

a. Make privacy notice(s) available to individuals upon first interacting with an organization, and subsequently [*Assignment: organization-defined frequency*]; and.

b. Ensure that privacy notices are clear and easy-to-understand, expressing information about personally identifiable information processing in plain language.

Supplemental Guidance: To help users understand how their information is being processed, organizations write materials in plain language and avoid technical jargon. When developing privacy notices, organizations consider the application of good information design procedures in all user-facing materials; use of active voice and conversational style; logical sequencing of main points; consistent use of the same word (rather than synonyms) to avoid confusion; use of bullets, numbers, and formatting where appropriate to aid readability; and legibility of text, such as font style, size, color, and contrast with surrounding background.

Related Controls: IP-2, IP-3, IP-4, IP-5, PA-2, PA-3, PA-4, PM-21.

Control Enhancements:

(1) PRIVACY NOTICE | JUST-IN-TIME NOTICE OF PRIVACY AUTHORIZATION

Present authorizations to process personally identifiable information in conjunction with the data action, or [*Assignment: organization-defined frequency*].

Supplemental Guidance: If the circumstances under which an individual gave consent have changed or a significant amount of time has passed since an individual gave consent for the

processing of his or her personally identifiable information, the data subject's assumption about how the information is being processed might no longer be accurate or reliable. Just-in-time notice can help maintain individual satisfaction with or ability to participate in how the personally identifiable information is being processed.

Related Controls: IP-2, IP-3, IP-5, PA-3, PA-4, PM-22.

References: NIST Interagency Report 8062.

IP-5 PRIVACY ACT STATEMENTS

Control:

a. Include Privacy Act Statements on organizational forms that collect personally identifiable information, or on separate forms that can be retained by individuals; or

b. Read a Privacy Act Statement to the individual prior to initiating the collection of personally identifiable information verbally.

Supplemental Guidance: Privacy Act Statements provide additional formal notice to individuals from whom the information is being collected, notice of the authority of organizations to collect personally identifiable information; whether providing personally identifiable information is mandatory or optional; the principal purpose or purposes for which the personally identifiable information is to be used; the intended disclosures or routine uses of the information; and the consequences of not providing all or some portion of the information requested. Personally identifiable information may be collected verbally, for example, when conducting telephone interviews or surveys.

Related Controls: IP-4, PA-3, PM-20, PM-21.

Control Enhancements: None.

References: None.

IP-6 INDIVIDUAL ACCESS

Control: Provide individuals the ability to access their personally identifiable information maintained in organizational systems of records.

Supplemental Guidance: Access affords individuals the ability to review personally identifiable information about them held within organizational systems of records. Access includes timely, simplified, and inexpensive access to data. Organizational processes for allowing access to records may differ based on resources, legal requirements, or other factors. The Senior Agency Official for Privacy is responsible for the content of Privacy Act regulations and record request processing, in consultation with legal counsel. Access to certain types of records may not be appropriate, and heads of agencies may promulgate rules exempting specific systems from the access provision of the Privacy Act. When feasible, those rules will be publicly available. In addition, individuals are not entitled to access to information compiled in reasonable anticipation of a civil action or proceeding.

Related Controls: IP-3, PA-3, PM-27.

Control Enhancements: None.

References: NIST Interagency Report 8062.

3.9 INCIDENT RESPONSE

Quick link to Incident Response summary table

IR-1 INCIDENT RESPONSE POLICY AND PROCEDURES

Control:

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

1. An 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 senior management official*] to manage the incident response policy and procedures;

~~b.~~c. Review and update the current incident response:

1. Policy [*Assignment: organization-defined frequency*]; and

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

d. Ensure that the incident response procedures implement the incident response policy and controls; and

e. Develop, document, and implement remediation actions for violations of the incident response policy.

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of ~~selected security~~ the controls and control enhancements in the IR family. The risk management strategy is an important factor in establishing policy and procedures ~~reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards,~~. Comprehensive policy and ~~guidance.~~procedures help provide security and privacy assurance. Security and privacy program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general ~~information~~ security and privacy policy ~~for organizations~~ or ~~conversely,~~ can be represented by multiple policies reflecting the complex nature of ~~certain~~ organizations. The procedures can be established for ~~the~~ security ~~program in general~~and privacy programs and for ~~particular information~~ systems, if needed. ~~The~~Procedures describe how policies or controls are implemented and can be directed at the personnel 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. It is important to recognize that restating controls does not constitute an organizational ~~risk management strategy is a key factor in establishing policy and procedures.~~ policy or procedure.

Related Controls: PM-9, PS-8, SI-12.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-30, 800-39, 800-61, 800-83, 800-100.

IR-2 INCIDENT RESPONSE TRAINING

Control: Provide incident response training to system users consistent with assigned roles and responsibilities:

a. Within [*Assignment: organization-defined time-period*] of assuming an incident response role or responsibility;

b. When required by system changes; and

c. [*Assignment: organization-defined frequency*] thereafter.

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

Related Controls: AT-2, AT-4, AT-3, CP-3, IR-3, IR-4, IR-8, IR-9.

Control Enhancements:

(1) INCIDENT RESPONSE TRAINING | SIMULATED EVENTS

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

Supplemental Guidance: None.

Related Controls: None.

(2) INCIDENT RESPONSE TRAINING | AUTOMATED TRAINING ENVIRONMENTS

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

Supplemental Guidance: None.

Related Controls: None.

References: NIST Special Publication 800-50.

IR-3 INCIDENT RESPONSE TESTING

Control: Test the incident response capability for the system [*Assignment: organization-defined frequency*] using [*Assignment: organization-defined tests*] to determine the incident response effectiveness and documents the results.

Supplemental Guidance: Organizations test incident response capabilities to determine the overall effectiveness of the capabilities and to identify potential weaknesses or deficiencies. Incident response testing includes, for example, the use of checklists, walk-through or tabletop exercises, simulations (parallel/full interrupt), and comprehensive exercises. Incident response testing can also include a determination of the effects on organizational operations, organizational assets, and individuals due to incident response. Use of qualitative and quantitative data aids in determining the effectiveness of incident response processes.

Related Controls: CP-3, CP-4, IR-2, IR-4, IR-8, PM-14.

Control Enhancements:

(1) INCIDENT RESPONSE TESTING | AUTOMATED TESTING

Employ automated mechanisms to more thoroughly and effectively test the incident response capability.

Supplemental Guidance: Organizations use automated mechanisms to more thoroughly and effectively test incident response capabilities. This can be accomplished, for example, by

providing more complete coverage of incident response issues; by selecting more realistic test scenarios and test environments; and by stressing the response capability.

Related Controls: None.

(2) INCIDENT RESPONSE TESTING | COORDINATION WITH RELATED PLANS

Coordinate incident response testing with organizational elements responsible for related plans.

Supplemental Guidance: Organizational plans related to incident response testing include, for example, Business Continuity Plans, Contingency Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Occupant Emergency Plans, and Critical Infrastructure Plans.

Related Controls: None.

(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 incorporating advanced information security practices; and

(c) Provide incident response measures and metrics that are accurate, consistent, and in a reproducible format.

Supplemental Guidance: To help incident response activities function as intended, organizations may use of 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.

Related Controls: None.

References: NIST Special Publications 800-84, 800-115.

IR-4 INCIDENT HANDLING

Control:

a. Implement an incident handling capability for security and privacy incidents that 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.

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

Related Controls: AC-19, AU-6, AU-7, CM-6, CP-2, CP-3, CP-4, IR-2, IR-3, IR-8, PE-6, PL-2, PM-12, SA-12, SC-5, SC-7, SI-3, SI-4, SI-7.

Control Enhancements:

(1) INCIDENT HANDLING | AUTOMATED INCIDENT HANDLING PROCESSES

Employ automated mechanisms to support the incident handling process.

Supplemental Guidance: Automated mechanisms supporting incident handling processes include, for example, online incident management systems; and tools that support collection of live response data, full network packet capture, and forensic analysis.

Related Controls: None.

(2) INCIDENT HANDLING | DYNAMIC RECONFIGURATION

Include dynamic reconfiguration of [*Assignment: organization-defined system components*] as part of the incident response capability.

Supplemental Guidance: Dynamic reconfiguration includes, for example, changes to router rules, access control lists, intrusion detection/prevention system parameters, and filter rules for firewalls and gateways. Organizations perform dynamic reconfiguration of systems, for example, to stop attacks, to misdirect attackers, and to isolate components of systems, thus limiting the extent of the damage from breaches or compromises. Organizations include time frames for achieving the reconfiguration of systems in the definition of the reconfiguration capability, considering the potential need for rapid response to effectively address ~~sophisticated~~ cyber threats.

Related Controls: AC-2, AC-4, CM-2.

(3) INCIDENT HANDLING | CONTINUITY OF OPERATIONS

Identify [*Assignment: organization-defined classes of incidents*] and [*Assignment: organization-defined actions to take in response to classes of incidents*] to ensure continuation of organizational missions and business functions.

Supplemental Guidance: Classes of incidents include, for example, malfunctions due to design/implementation errors and omissions, targeted malicious attacks, and untargeted malicious attacks. Appropriate incident response actions include, for example, graceful degradation, system shutdown, fall back to manual mode/alternative technology whereby the system operates differently, employing deceptive measures, alternate information flows, or operating in a mode that is reserved solely for when systems are under attack.

Related Controls: None.

(4) INCIDENT HANDLING | INFORMATION CORRELATION

Correlate incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.

Supplemental Guidance: Sometimes the nature of a threat event, for example, a hostile attack, is such that it can only be observed by bringing together information from different sources including various reports and reporting procedures established by organizations.

Related Controls: None.

(5) INCIDENT HANDLING | AUTOMATIC DISABLING OF SYSTEM

Implement a configurable capability to automatically disable the system if [*Assignment: organization-defined security violations*] are detected.

Supplemental Guidance: None.

Related Controls: None.

(6) INCIDENT HANDLING | INSIDER THREATS — SPECIFIC CAPABILITIES

Implement an incident handling capability for incidents involving insider threats.

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

Related Controls: None.

(7) INCIDENT HANDLING | INSIDER THREATS — INTRA-ORGANIZATION COORDINATION

Coordinate an incident handling capability for insider threats across [*Assignment: organization-defined components or elements of the organization*].

Supplemental Guidance: Incident handling for insider threat incidents (including preparation, detection and analysis, containment, eradication, and recovery) requires close coordination

among a variety of organizational components or elements to be effective. These components or elements include, for example, mission/business owners, system owners, human resources offices, procurement offices, personnel/physical security offices, operations personnel, and risk executive (function). In addition, organizations may require external support from federal, state, and local law enforcement agencies.

Related Controls: None.

(8) INCIDENT HANDLING | CORRELATION WITH EXTERNAL ORGANIZATIONS

Coordinate with [*Assignment: organization-defined external organizations*] to correlate and share [*Assignment: organization-defined incident information*] to achieve a cross-organization perspective on incident awareness and more effective incident responses.

Supplemental Guidance: The coordination of incident information with external organizations including, for example, mission/business partners, military/coalition partners, customers, and multi-tiered developers, can provide significant benefits. Cross-organizational coordination with respect to incident handling can serve as an important risk management capability. This capability allows organizations to leverage critical information from a variety of sources to effectively respond to information security-related incidents potentially affecting the organization's operations, assets, and individuals.

Related Controls: AU-16, PM-16.

(9) INCIDENT HANDLING | DYNAMIC RESPONSE CAPABILITY

Employ [*Assignment: organization-defined dynamic response capabilities*] to effectively respond to security incidents.

Supplemental Guidance: This control enhancement addresses the timely deployment of new or replacement organizational capabilities in response to security and privacy incidents ~~(e.g., adversary actions during hostile cyber attacks).~~. This includes capabilities implemented at the mission and business process level ~~(e.g., activating alternative mission/business processes)~~ and at the system level.

Related Controls: None.

(10) INCIDENT HANDLING | SUPPLY CHAIN COORDINATION

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

Supplemental Guidance: Organizations involved in supply chain activities include, for example, system/product developers, integrators, manufacturers, packagers, assemblers, distributors, vendors, and resellers. Supply chain incidents include, for example, compromises/breaches involving system components, information technology products, development processes or personnel, and distribution processes or warehousing facilities.

Related Controls: MA-2, SA-9.

References: NIST Special Publications 800-61, 800-101, 800-86; NIST Interagency Report 7599.

IR-5 INCIDENT MONITORING

Control: Track and document system security and privacy incidents.

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

Related Controls: AU-6, AU-7, IR-8, PE-6, PM-29, SC-5, SC-7, SI-3, SI-4, SI-7.

Control Enhancements:

(1) INCIDENT MONITORING | AUTOMATED TRACKING, DATA COLLECTION, AND ANALYSIS

Employ automated mechanisms to assist in the tracking of security and privacy incidents and in the collection and analysis of incident information.

Supplemental Guidance: Automated mechanisms for tracking incidents and for collecting and analyzing incident information include, for example, ~~the Einstein network monitoring device and monitoring online~~ Computer Incident Response Centers or other electronic databases of incidents and network monitoring devices.

Related Controls: AU-7, IR-4.

References: NIST Special Publication 800-61.

IR-6 INCIDENT REPORTING

Control:

a. Require personnel to report suspected security and privacy incidents to the organizational incident response capability within [*Assignment: organization-defined time-period*]; and

b. Report security, privacy, and supply chain incident information to [*Assignment: organization-defined authorities*].

Supplemental Guidance: The intent of this control is to address both specific incident reporting requirements within an organization and the ~~formal~~ incident reporting requirements for ~~federal agencies and their subordinate~~ organizations. Suspected security incidents include, for example, the receipt of suspicious email communications that can potentially contain malicious code. ~~The types of security~~Suspected privacy incidents include, for example a suspected breach of personally identifiable information or the recognition that the processing of personally identifiable information creates potential privacy risk. The types of incidents reported, the content and timeliness of the reports, and the designated reporting authorities reflect applicable ~~federal~~ laws, Executive Orders, directives, regulations, policies, standards, and ~~guidance. Current federal policy requires that all federal agencies (unless specifically exempted from such requirements) report security incidents to the United States Computer Emergency Readiness Team (US-CERT) within specified time frames designated in the US-CERT~~ guidelines~~Concept of Operations for Federal Cyber Security Incident Handling~~.

Related Controls: CM-6, CP-2, IR-4, IR-5, IR-8, IR-9.

Control Enhancements:

(1) INCIDENT REPORTING | AUTOMATED REPORTING

Employ automated mechanisms to assist in the reporting of security and privacy incidents.

Supplemental Guidance: None.

Related Controls: IR-7.

(2) INCIDENT REPORTING | VULNERABILITIES RELATED TO INCIDENTS

Report system vulnerabilities associated with reported security and privacy incidents to [*Assignment: organization-defined personnel or roles*].

Supplemental Guidance: None.

Related Controls: None.

(3) INCIDENT REPORTING | ~~*COORDINATION WITH*~~ SUPPLY CHAIN COORDINATION

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

Supplemental Guidance: Organizations involved in supply chain activities include, for example, system/product developers, integrators, manufacturers, packagers, assemblers, distributors, vendors, and resellers. Supply chain incidents include, for example, compromises/breaches involving system components, information technology products, development processes or personnel, and distribution processes or warehousing facilities. Organizations determine the appropriate information to share considering the value gained from support by external

organizations with the potential for harm due to ~~sensitive~~controlled unclassified information being released to outside organizations of perhaps questionable trustworthiness.

Related Controls: SA-12.

References: NIST Special Publication 800-61.

IR-7 INCIDENT RESPONSE ASSISTANCE

Control: Provide an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the system for the handling and reporting of security and privacy incidents.

Supplemental Guidance: Incident response support resources provided by organizations include, for example, help desks, assistance groups, and access to forensics services or consumer redress services, when required.

Related Controls: AT-2, AT-3, IP-3, IR-4, IR-6, IR-8, PM-28, SA-9.

Control Enhancements:

(1) INCIDENT RESPONSE ASSISTANCE | AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION AND SUPPORT

Employ automated mechanisms to increase the availability of incident response-related information and support.

Supplemental Guidance: Automated mechanisms can provide a push and/or pull capability for users to obtain incident response assistance. For example, individuals might have access to a website to query the assistance capability, or ~~conversely,~~ the assistance capability ~~may have the ability to~~can proactively send information to users (general distribution or targeted) as part of increasing understanding of current response capabilities and support.

Related Controls: None.

(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.

Supplemental Guidance: External providers of a system protection capability include, for example, 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.

Related Controls: None.

References: NIST Interagency Report 7559.

IR-8 INCIDENT RESPONSE PLAN

Control:

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. Is reviewed and approved by [*Assignment: organization-defined personnel or roles*] [*Assignment: organization-defined frequency*]; and

9. 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. Reviews the incident response plan [*Assignment: organization-defined frequency*];~~

~~d.~~c. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing;

~~e.~~d. Communicate incident response plan changes to [*Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements*]; and

~~f.~~e. Protect the incident response plan from unauthorized disclosure and modification.

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

Related Controls: AC-2, CP-2, CP-4, IR-4, IR-7, IR-9, PE-6, PL-2, SA-12, SA-15, SI-12.

Control Enhancements:

(1) INCIDENT RESPONSE PLAN | PERSONALLY IDENTIFIABLE INFORMATION PROCESSES

Include the following additional processes in the Incident Response Plan for incidents involving personally identifiable information:

(a) A process to determine if notice to oversight organizations is appropriate and to provide that notice, if appropriate;

(b) An assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals; and

(c) A process to ensure prompt reporting by organizational users of any privacy incident to [*Assignment: organization-defined roles*].

Supplemental Guidance: Some organizations may be required by law or policy to provide notice to oversight organizations in the event of a privacy-related incident. Organization-defined roles to which privacy incidents may be reported include, for example, the Senior Agency Official for Privacy, Senior Agency Information Security Officer, Authorizing Official, and System Owner.

Related Controls: None.

References: NIST Special Publication 800-61.

IR-9 INFORMATION SPILLAGE RESPONSE

Control: Respond to information spills by:

~~b.~~a. Identifying the specific information involved in the system contamination;

~~c.~~b. Alerting [*Assignment: organization-defined personnel or roles*] of the information spill using a method of communication not associated with the spill;

~~d.~~c. Isolating the contaminated system or system component;

~~e.~~d. Eradicating the information from the contaminated system or component;

~~f.~~e. Identifying other systems or system components that may have been subsequently contaminated; and

~~g.~~f. Performing ~~other~~the following additional actions: [*Assignment: organization-defined actions*].

Supplemental Guidance: Information spillage refers to instances where either classified or ~~sensitive~~controlled unclassified information is inadvertently placed on systems that are not authorized to process such information. Such information spills occur when information that is initially thought to be of lower sensitivity is transmitted to a system and then subsequently determined to be of higher sensitivity. At that point, corrective action is required. The nature of the organizational response is generally based upon the degree of sensitivity of the spilled information ~~(e.g., security category or classification level),~~ the security capabilities of the system, the specific nature of contaminated storage media, and the access authorizations ~~(e.g., security clearances)~~ of individuals with authorized access to the contaminated system. The methods used to communicate information about the spill after the fact do not involve methods directly associated with the actual spill to minimize the risk of further spreading the contamination before such contamination is isolated and eradicated.

Related Controls: CP-2, IR-6, PM-28, PM-30, RA-7.

Control Enhancements:

(1) INFORMATION SPILLAGE RESPONSE | RESPONSIBLE PERSONNEL

Assign [*Assignment: organization-defined personnel or roles*] with responsibility for responding to information spills.

Supplemental Guidance: None.

Related Controls: None.

(2) INFORMATION SPILLAGE RESPONSE | TRAINING

Provide information spillage response training [*Assignment: organization-defined frequency*].

Supplemental Guidance: None.

Related Controls: AT-2, AT-3, CP-3, IR-2.

(3) INFORMATION SPILLAGE RESPONSE | POST-SPILL OPERATIONS

Implement [*Assignment: organization-defined procedures*] to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions.

Supplemental Guidance: Correction actions for systems contaminated due to information spillages may be very time-consuming. During those periods, personnel may not have access to the contaminated systems, which may potentially affect their ability to conduct organizational business.

Related Controls: None.

(4) INFORMATION SPILLAGE RESPONSE | EXPOSURE TO UNAUTHORIZED PERSONNEL

Employ [*Assignment: organization-defined security safeguards*] for personnel exposed to information not within assigned access authorizations.

Supplemental Guidance: Security safeguards include, for example, ensuring that personnel who are exposed to spilled information are made aware of the ~~federal~~ laws, Executive Orders, directives, regulations, policies, standards, and~~/or regulations~~ guidelines regarding the information and the restrictions imposed based on exposure to such information.

Related Controls: None.

References: None.

IR-10 INTEGRATED INFORMATION SECURITY ANALYSIS TEAM

Control: Establish an integrated team of forensic and malicious code analysts, tool developers, and real-time operations personnel to handle incidents.

Supplemental Guidance: Having an integrated team for incident response facilitates information sharing. Such capability allows organizational personnel, including developers, implementers, and operators, to leverage the team knowledge of the threat to implement defensive measures that will enable organizations to deter intrusions more effectively. Moreover, integrated teams promote the rapid detection of intrusions, development of appropriate mitigations, and the deployment of effective defensive measures. For example, when an intrusion is detected, the integrated analysis team can rapidly develop an appropriate response for operators to implement, correlate the new incident with information on past intrusions, and augment ongoing intelligence development. This enables the team to identify adversary ~~TTPs~~tactics, techniques, and procedures that are linked to the operations tempo or to specific missions and business functions, and to define responsive actions in a way that does not disrupt those missions and business ~~operations. Ideally,~~functions. Information security analysis teams are distributed within organizations to make the capability more resilient.

Related Controls: AT-3.

Control Enhancements: None.

References: NIST Special Publication 800-150; NIST Interagency Report 7559.

3.10 MAINTENANCE

Quick link to Maintenance summary table

MA-1 SYSTEM MAINTENANCE POLICY AND PROCEDURES

Control:

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

1. A system 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 system maintenance policy and the associated system maintenance controls;

b. Designate an [*Assignment: organization-defined senior management official*] to manage the system maintenance policy and procedures;

~~b.~~c. Review and update the current system maintenance:

1. Policy [*Assignment: organization-defined frequency*]; and

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

d. Ensure that the system maintenance procedures implement the system maintenance policy and controls; and

e. Develop, document, and implement remediation actions for violations of the maintenance policy.

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of ~~selected security~~ the controls and control enhancements in the MA family. The risk management strategy is an important factor in establishing policy and procedures ~~reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards,~~. Comprehensive policy and ~~guidance.~~procedures help provide security and privacy assurance. Security and privacy program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general ~~information~~ security and privacy policy ~~for organizations~~ or ~~conversely,~~ can be represented by multiple policies reflecting the complex nature of ~~certain~~ organizations. The procedures can be established for ~~the~~ security ~~program in general~~and privacy programs and for ~~particular information~~ systems, if needed. ~~The~~Procedures describe how policies or controls are implemented and can be directed at the personnel 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. It is important to recognize that restating controls does not constitute an organizational ~~risk management strategy is a key factor in establishing policy and procedures.~~ policy or procedure.

Related Controls: PM-9, PS-8, SI-12.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-30, 800-39, 800-100.

MA-2 CONTROLLED MAINTENANCE

Control:

a. Schedule, document, and review records of maintenance ~~and repairs~~, repair, or 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 ~~equipment is~~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 all information from associated media prior to removal from organizational facilities for off-site maintenance, repair, or replacement;

e. Check all potentially impacted security and privacy controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions; and

f. Include [*Assignment: organization-defined maintenance-related information*] in organizational maintenance records.

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

Related Controls: CM-3, CM-4, CM-5, MA-4, MP-6, PE-16, SA-12, SA-19, SI-2.

Control Enhancements:

(1) CONTROLLED MAINTENANCE | RECORD CONTENT

[Withdrawn: Incorporated into MA-2].

(2) CONTROLLED MAINTENANCE | AUTOMATED MAINTENANCE ACTIVITIES

(a) Employ automated mechanisms to schedule, conduct, and document maintenance, repair, and replacement actions for the system or system components; and

(b) Produce up-to date, accurate, and complete records of all maintenance, repair, and replacement actions requested, scheduled, in process, and completed.

Supplemental Guidance: None.

Related Controls: MA-3.

References: NIST Interagency Report 8023.

MA-3 MAINTENANCE TOOLS

Control:

a. Approve, control, and monitor the use of system maintenance tools; and

b. Review previously approved system maintenance tools [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses security-related issues associated with maintenance tools that are not within organizational system boundaries but are used specifically for diagnostic and repair actions on organizational systems. Organizations have flexibility in determining roles

for approval of maintenance tools and how that approval is documented. Periodic review of system maintenance tools facilitates withdrawal of the approval for outdated, unsupported, irrelevant, or no-longer-used tools. Maintenance tools can include hardware, software, and firmware items. Maintenance tools are potential vehicles for transporting malicious code, intentionally or unintentionally, into a facility and subsequently into systems. Maintenance tools can include, for example, hardware/software diagnostic test equipment and hardware and software packet sniffers. This control does not cover hardware or software components that support system maintenance and are a part of the system, for example, the software implementing "ping," "ls," "ipconfig," or the hardware and software implementing the monitoring port of an Ethernet switch.

Related Controls: MA-2, PE-16.

Control Enhancements:

(1) MAINTENANCE TOOLS | INSPECT TOOLS

Inspect the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.

Supplemental Guidance: If, upon inspection of maintenance tools, organizations determine that the tools have been modified in an improper/unauthorized manner or contain malicious code, the incident is handled consistent with organizational policies and procedures for incident handling.

Related Controls: SI-7.

(2) MAINTENANCE TOOLS | INSPECT MEDIA

Check media containing diagnostic and test programs for malicious code before the media are used in the system.

Supplemental Guidance: If, upon inspection of media containing maintenance diagnostic and test programs, organizations determine that the media contain malicious code, the incident is handled consistent with organizational incident handling policies and procedures.

Related Controls: SI-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.

Supplemental Guidance: Organizational information includes all information specifically owned by organizations and information provided to organizations in which organizations serve as information stewards.

Related Controls: MP-6.

(4) MAINTENANCE TOOLS | RESTRICTED TOOL USE

Restrict the use of maintenance tools to authorized personnel only.

Supplemental Guidance: This control enhancement applies to systems that are used to carry out maintenance functions.

Related Controls: AC-3, AC-5, AC-6.

References: NIST Special Publication 800-88.

MA-4 NONLOCAL MAINTENANCE

Control:

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 authenticators 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.

Supplemental Guidance: Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through a network, either an external network ~~(e.g., the Internet)~~ or an internal network. Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the system or system component and not communicating across a network connection. Authentication techniques used in the establishment of nonlocal maintenance and diagnostic sessions reflect the network access requirements in IA-2. Strong authentication requires authenticators that are resistant to replay attacks and employ multifactor authentication. Strong authenticators include, for example, PKI where certificates are stored on a token protected by a password, passphrase, or biometric. Enforcing requirements in MA-4 is accomplished in part by other controls.

Related Controls: 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.

Control Enhancements:

(1) NONLOCAL MAINTENANCE | AUDITING AND REVIEW

(a) Audit [*Assignment: organization-defined audit events*] for nonlocal maintenance and diagnostic sessions; and

(b) Review the records of the maintenance and diagnostic sessions.

Supplemental Guidance: None.

Related Controls: AU-6, AU-12.

(2) NONLOCAL MAINTENANCE | DOCUMENT NONLOCAL MAINTENANCE

~~**The organization documents in the security plan for the information system, the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.**~~

[Withdrawn: Incorporated into MA-1 and 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) before removal from organizational facilities; and after the service is performed, inspect and sanitize the component (for potentially malicious software) before reconnecting the component to the system.

Supplemental Guidance: Comparable security capability on systems, diagnostic tools, and equipment providing maintenance services implies that the implemented security controls on those systems, tools, and equipment are at least as comprehensive as the controls on the system being serviced.

Related Controls: MP-6, SI-3, SI-7.

(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 based upon encryption.

Supplemental Guidance: None.

Related Controls: None.

(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 [*Assignment: organization-defined personnel or roles*] of the date and time of planned nonlocal maintenance.

Supplemental Guidance: Notification may be performed by maintenance personnel. Approval of nonlocal maintenance sessions is accomplished by organizational personnel with sufficient information security and system knowledge to determine the appropriateness of the proposed maintenance.

Related Controls: None.

(6) NONLOCAL MAINTENANCE | CRYPTOGRAPHIC PROTECTION

Implement cryptographic mechanisms to protect the integrity and confidentiality of nonlocal maintenance and diagnostic communications.

Supplemental Guidance: None.

Related Controls: SC-8, SC-13.

(7) NONLOCAL MAINTENANCE | REMOTE DISCONNECT VERIFICATION

Implement remote disconnect verification at the termination of nonlocal maintenance and diagnostic sessions.

Supplemental Guidance: Remote disconnect verification ensures that remote connections from nonlocal maintenance sessions have been terminated and are no longer available for use.

Related Controls: AC-12.

References: FIPS Publications 140-2, 197, 201; NIST Special Publications 800-63, 800-88.

MA-5 MAINTENANCE PERSONNEL

Control:

a. Establish a process for maintenance personnel authorization and maintains 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.

Supplemental Guidance: This control applies to individuals performing hardware or software maintenance on organizational systems, while PE-2 addresses physical access for individuals whose maintenance duties place them within the physical protection perimeter of the systems ~~(e.g., custodial staff, physical plant maintenance personnel).~~ Technical competence of supervising individuals relates to the maintenance performed on the systems while having required access authorizations refers to maintenance on and near the systems. Individuals not previously identified as authorized maintenance personnel, such as information technology manufacturers, vendors, systems integrators, and consultants, may require privileged access to organizational systems, for example, when required to conduct maintenance activities with little or no notice. Based on organizational assessments of risk, organizations may issue temporary credentials to these individuals. Temporary credentials may be for one-time use or for very limited time-periods.

Related Controls: AC-2, AC-3, AC-5, AC-6, IA-2, IA-8, MA-4, MP-2, PE-2, PE-3, PS-7, RA-3.

Control Enhancements:

(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;

(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 alternate security safeguards in the event a system component cannot be sanitized, removed, or disconnected from the system.

Supplemental Guidance: This control enhancement denies individuals who lack appropriate security clearances ~~(i.e., individuals who do not possess security clearances or possess security clearances at a lower level than required)~~ or who are not U.S. citizens, visual and electronic access to any classified or controlled unclassified information contained on organizational systems. Procedures for the use of maintenance personnel can be documented in security plans for the systems.

Related Controls: MP-6, PL-2.

(2) MAINTENANCE PERSONNEL | SECURITY CLEARANCES FOR CLASSIFIED SYSTEMS

Verify that personnel performing maintenance and diagnostic activities on a system processing, storing, or transmitting classified information possess security clearances and formal access approvals for at least the highest classification level and for all compartments of information on the system.

Supplemental Guidance: None.

Related Controls: PS-3.

(3) MAINTENANCE PERSONNEL | CITIZENSHIP REQUIREMENTS FOR CLASSIFIED SYSTEMS

Verify that personnel performing maintenance and diagnostic activities on a system processing, storing, or transmitting classified information are U.S. citizens.

Supplemental Guidance: None.

Related Controls: PS-3.

(4) MAINTENANCE PERSONNEL | FOREIGN NATIONALS

Verify that:

(a) Foreign nationals with appropriate security clearances are used to conduct maintenance and diagnostic activities on classified systems only when the systems are jointly owned and operated by the United States and foreign allied governments, or owned and operated solely by foreign allied governments; and

(b) Approvals, consents, and detailed operational conditions regarding the use of foreign nationals to conduct maintenance and diagnostic activities on classified systems are fully documented within Memoranda of Agreements.

Supplemental Guidance: None.

Related Controls: PS-3.

(5) MAINTENANCE PERSONNEL | ~~*NONSYSTEM-RELATED*~~ NON-SYSTEM MAINTENANCE

Verify that non-escorted personnel performing maintenance activities not directly associated with the system but in the physical proximity of the system, have required access authorizations.

Supplemental Guidance: Personnel performing maintenance activities in other capacities not directly related to the system include, for example, physical plant personnel and janitorial personnel.

Related Controls: None.

References: None.

MA-6 TIMELY MAINTENANCE

Control: Obtain maintenance support and/or spare parts for [*Assignment: organization-defined system components*] within [*Assignment: organization-defined time-period*] of failure.

Supplemental Guidance: Organizations specify the system components that result in increased risk to organizational operations and assets, individuals, other organizations, or the Nation when the

functionality provided by those components is not operational. Organizational actions to obtain maintenance support typically include having appropriate contracts in place.

Related Controls: CM-8, CP-2, CP-7, RA-7, SA-12, SA-15, SI-13.

Control Enhancements:

(1) TIMELY MAINTENANCE | PREVENTIVE MAINTENANCE

Perform preventive maintenance on [*Assignment: organization-defined system components*] at [*Assignment: organization-defined time intervals*].

Supplemental Guidance: Preventive maintenance includes proactive care and servicing of system components to maintain 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/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, for example, original equipment manufacturer recommendations, statistical failure records, requirements of codes, legislation, or regulations within a jurisdiction, expert opinion, maintenance that has already been conducted on similar equipment, or measured values and performance indications.

Related Controls: None.

(2) TIMELY MAINTENANCE | PREDICTIVE MAINTENANCE

Perform predictive maintenance on [*Assignment: organization-defined system components*] at [*Assignment: organization-defined time intervals*].

Supplemental Guidance: Predictive maintenance, or condition-based maintenance, attempts to evaluate 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 point in 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 goal of predicting the future trend of the equipment's condition. This approach uses 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, thereby minimizing disruption of normal system operations. Predictive maintenance can result in substantial cost savings and higher system reliability. Predictive maintenance tends to include measurement of the item. To evaluate equipment condition, predictive maintenance utilizes nondestructive testing technologies such as infrared, acoustic (partial discharge and airborne ultrasonic), corona detection, vibration analysis, sound level measurements, oil analysis, and other specific online tests.

Related Controls: None.

(3) TIMELY MAINTENANCE | AUTOMATED SUPPORT FOR PREDICTIVE MAINTENANCE

Employ automated mechanisms to transfer predictive maintenance data to a computerized maintenance management system.

Supplemental Guidance: A computerized maintenance management system maintains a ~~computer~~ database of information about the maintenance operations of organizations and automates processing equipment condition data to trigger maintenance planning, execution, and reporting.

Related Controls: None.

(4) TIMELY MAINTENANCE | ADEQUATE SUPPLY

Employ [*Assignment: organization-defined security safeguards*] to ensure an adequate supply of [*Assignment: organization-defined critical system components*].

Supplemental Guidance: Adversaries can attempt to impede organizational operations by disrupting the supply of critical system components or corrupting supplier operations. Organizations may track systems and component mean time to failure to mitigate the loss of

temporary or permanent system function. Safeguards to ensure that adequate supplies of critical system components include, for example, the use of multiple suppliers throughout the supply chain for the identified critical components; stockpiling spare components to ensure operation during mission-critical times, and the identification of functionally-identical or similar components which may be used, if necessary.

Related Controls: SA-12, SA-19.

References: None.

3.11 MEDIA PROTECTION

Quick link to Media Protection summary table

MP-1 MEDIA PROTECTION POLICY AND PROCEDURES

Control:

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

1. A 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 senior management official*] to manage the media protection policy and procedures;

~~b.~~c. Review and update the current media protection:

1. Policy [*Assignment: organization-defined frequency*]; and

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

d. Ensure that the media protection procedures implement the media protection policy and controls; and

e. Develop, document, and implement remediation actions for violations of the media protection policy.

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of ~~selected security~~ the controls and control enhancements in the MP family. The risk management strategy is an important factor in establishing policy and procedures ~~reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards,~~. Comprehensive policy and ~~guidance.~~procedures help provide security and privacy assurance. Security and privacy program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general ~~information~~ security and privacy policy ~~for organizations~~ or ~~conversely,~~ can be represented by multiple policies reflecting the complex nature of ~~certain~~ organizations. The procedures can be established for ~~the~~ security ~~program in general~~and privacy programs and for ~~particular information~~ systems, if needed. ~~The organizational risk management strategy is a key factor in establishing policy and procedures. Related control:~~Procedures describe how policies or controls are implemented and can be directed at the personnel 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. It is important to recognize that restating controls does not constitute an organizational policy or procedure.

Related Controls: PM-9, PS-8, SI-12.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-30, 800-39, 800-100.

MP-2 MEDIA ACCESS

Control: Restrict access to [*Assignment: organization-defined types of digital and/or non-digital media*] to [*Assignment: organization-defined personnel or roles*].

Supplemental Guidance: System media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Restricting non-digital media access includes, for example, denying access to patient medical records in a community hospital unless the individuals seeking access to such records are authorized healthcare providers. Restricting access to digital media includes, for example, limiting access to design specifications stored on compact disks in the media library to the project leader and the individuals on the development team.

Related Controls: AC-19, AU-9, CP-2, CP-9, CP-10, MA-5, MP-6, MP-4, PE-2, PE-3, SC-13, SC-34, SI-12.

Control Enhancements:

(1) MEDIA ACCESS | AUTOMATED RESTRICTED ACCESS

[Withdrawn: Incorporated into MP-4(2)].

(2) MEDIA ACCESS | CRYPTOGRAPHIC PROTECTION

[Withdrawn: Incorporated into SC-28(1)].

References: FIPS Publication 199; NIST Special Publication 800-111.

MP-3 MEDIA MARKING

Control:

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*].

Supplemental Guidance: Security marking refers to the application or use of human-readable security attributes. Security labeling refers to the application or use of security attributes regarding internal data structures within systems ~~(see AC-16). Information.~~ System media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external or removable~~hard~~ disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Security marking is generally not required for media containing information determined by organizations to be in the public domain or to be publicly releasable. However, some organizations may require markings for public information indicating that the information is publicly releasable. Marking of system media reflects applicable ~~federal~~ laws, Executive Orders, directives, policies, regulations, standards, and ~~guidance.~~ guidelines.

Related Controls: AC-16, CP-9, MP-5, PE-22, SI-12.

Control Enhancements: None.

References: FIPS Publication 199.

MP-4 MEDIA STORAGE

Control:

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 until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

Supplemental Guidance: System media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external or removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Physically controlling system media includes, for example, conducting inventories, ensuring procedures are in place to allow individuals to check out and return media to the media library, and maintaining accountability for stored media. Secure storage includes, for example, a locked drawer, desk, or cabinet; or a controlled media library. The type of media storage employed by organizations is commensurate with the security category or classification of the information residing on the media. Controlled areas are areas that provide sufficient physical and procedural safeguards to meet the requirements established for protecting information and systems. For media containing information determined to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on organizations or individuals if accessed by other than authorized personnel, fewer safeguards may be needed. In these situations, physical access controls provide adequate protection.

Related Controls: AC-19, CP-2, CP-6, CP-9, CP-10, MP-2, MP-7, PE-3, PL-2, SC-13, SC-28, SC-34, SI-12.

Control Enhancements:

(1) MEDIA STORAGE | CRYPTOGRAPHIC PROTECTION

[Withdrawn: Incorporated into SC-28(1)].

(2) MEDIA STORAGE | AUTOMATED RESTRICTED ACCESS

Employ automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted.

Supplemental Guidance: Automated mechanisms can include, for example, keypads or card readers on the external entries to media storage areas.

Related Controls: AC-3, AU-2, AU-6, AU-9, AU-12, PE-3.

References: FIPS Publication 199; NIST Special Publications 800-56A, 800-56B, 800-56C, 800-57-1, 800-57-2, 800-57-3, 800-111.

MP-5 MEDIA TRANSPORT

Control:

a. Protect and control [*Assignment: organization-defined types of system media*] during transport outside of controlled areas using [*Assignment: organization-defined security safeguards*];

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.

Supplemental Guidance: System media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, microfilm and paper. ~~This control also applies to mobile devices with information storage capability (e.g., smart phones, tablets, E-readers), that are transported outside of controlled areas.~~ Controlled areas are areas or spaces for which organizations provide sufficient physical or procedural safeguards to meet requirements established for protecting information and systems.

Physical and technical safeguards for media are commensurate with the security category or classification of the information residing on the media. Safeguards to protect media during transport include, for example, locked containers and cryptography. Cryptographic mechanisms can provide confidentiality and integrity protections depending upon the mechanisms used. Activities associated with transport include the actual transport as well as those activities such as releasing media for transport and ensuring that media enters the appropriate transport processes. For the actual transport, authorized transport and courier personnel may include individuals from outside the organization ~~(e.g., U.S. Postal Service or a commercial transport or delivery service).~~.

Maintaining accountability of media during transport includes, for example, restricting transport activities to authorized personnel, and tracking and/or obtaining explicit records of transport activities as the media moves through the transportation system to prevent and detect loss, destruction, or tampering. Organizations establish documentation requirements for activities associated with the transport of system media in accordance with organizational assessments of risk to include the flexibility to define different record-keeping methods for the different types of media transport as part of an overall system of transport-related records.

Related Controls: AC-7, AC-19, CP-2, CP-9, MP-3, MP-4, PE-16, PL-2, SC-13, SC-28, SC-34.

Control Enhancements:

(1) MEDIA TRANSPORT | PROTECTION OUTSIDE OF CONTROLLED AREAS

[Withdrawn: Incorporated into MP-5].

(2) MEDIA TRANSPORT | DOCUMENTATION OF ACTIVITIES

[Withdrawn: Incorporated into MP-5].

(3) MEDIA TRANSPORT | CUSTODIANS

Employ an identified custodian during transport of system media outside of controlled areas.

Supplemental Guidance: 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 at all times.

Related Controls: None.

(4) MEDIA TRANSPORT | CRYPTOGRAPHIC PROTECTION

~~**The information system implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.**~~

~~Supplemental Guidance: This control enhancement applies to both portable storage devices (e.g., USB memory sticks, compact disks, digital video disks, external/removable hard disk drives) and mobile devices with storage capability (e.g., smart phones, tablets, E-readers). Related control: MP-2.~~

[Withdrawn: Incorporated into SC-28(1)].

References: FIPS Publication 199; NIST Special Publication 800-60-1, 800-60-2.

MP-6 MEDIA SANITIZATION

Control:

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*~~] in accordance with applicable federal and organizational standards and policies;~~]; and

b. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

Supplemental Guidance: This control applies to all system media, both digital and non-digital, subject to disposal or reuse, whether or not the media is considered removable. Examples include: digital media found in scanners, copiers, printers, notebook computers, workstations, network components, mobile devices; and non-digital media such as paper and microfilm. The sanitization process removes information from the media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erase, and destruction, prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal. Organizations determine the appropriate sanitization methods recognizing that destruction is sometimes necessary when other methods cannot be applied to media requiring sanitization. Organizations use discretion on the employment of approved sanitization techniques and procedures for media containing information deemed to be in the public domain or publicly releasable, or deemed to have no adverse impact on organizations or

individuals if released for reuse or disposal. Sanitization of non-digital media includes, for example, destruction, removing a classified appendix from an otherwise unclassified document, or redacting selected sections or words from a document by obscuring the redacted sections or words in a manner equivalent in effectiveness to removing them from the document. NARA policy and guidance control the sanitization process for controlled unclassified information. NSA standards and policies control the sanitization process for media containing classified information.

Related Controls: AC-3, AC-7, AU-11, MA-2, MA-3, MA-4, MA-5, SI-12, SI-18.

Control Enhancements:

(1) MEDIA SANITIZATION | REVIEW, APPROVE, TRACK, DOCUMENT, AND VERIFY

Review, approve, track, document, and verify media sanitization and disposal actions.

Supplemental Guidance: Organizations review and approve media to be sanitized to ensure compliance with records-retention policies. Tracking and documenting actions include, for example, listing personnel who reviewed and approved sanitization and disposal actions; types of media sanitized; specific files stored on the media; sanitization methods used; date and time of the sanitization actions; personnel who performed the sanitization; verification actions taken; personnel who performed the verification; and the disposal actions taken. Organizations verify that the sanitization of the media was effective prior to disposal.

Related Controls: None.

(2) MEDIA SANITIZATION | EQUIPMENT TESTING

Test sanitization equipment and procedures [*Assignment: organization-defined frequency*] to verify that the intended sanitization is being achieved.

Supplemental Guidance: Testing of sanitization equipment and procedures may be conducted by qualified and authorized external entities including, for example, federal agencies or external service providers.

Related Controls: None.

(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*].

Supplemental Guidance: ~~This control enhancement applies to digital media containing classified information and Controlled Unclassified Information (CUI).~~ Portable storage devices can be the source of malicious code insertions into organizational systems. Many of these devices are obtained from ~~unknown and potentially~~ untrustworthy sources and may contain malicious code that can be readily transferred to systems through USB ports or other entry portals. While scanning ~~such~~ storage devices is ~~always~~ recommended, sanitization provides additional assurance that such devices are free of malicious code ~~to include code capable of initiating zero-day attacks.~~. Organizations consider nondestructive sanitization of portable storage devices when ~~such~~these devices are ~~first~~ purchased from manufacturers or vendors prior to initial use or when organizations ~~lose~~cannot maintain a positive chain of custody for the devices.

Related ~~control: SI-3~~Controls: None.

(4) MEDIA SANITIZATION | CONTROLLED UNCLASSIFIED INFORMATION

~~**(1)** *MEDIA SANITIZATION | CLASSIFIED INFORMATION*~~

[Withdrawn: Incorporated into MP-6].

(5) MEDIA SANITIZATION | ~~*MEDIA DESTRUCTION*~~CLASSIFIED INFORMATION

[Withdrawn: Incorporated into MP-6].

(6) MEDIA SANITIZATION | MEDIA DESTRUCTION

[Withdrawn: Incorporated into MP-6].

~~**(6)**~~**(7)** MEDIA SANITIZATION | DUAL AUTHORIZATION

Enforce dual authorization for the sanitization of [*Assignment: organization-defined system media*].

Supplemental Guidance: Organizations employ dual authorization to ensure that system media sanitization cannot occur unless two technically qualified individuals conduct the designated task. Individuals sanitizing system media possess sufficient skills and expertise to determine if the proposed sanitization reflects applicable federal and organizational standards, policies, and procedures. Dual authorization also helps to ensure that sanitization occurs as intended, both protecting against errors and false claims of having performed the sanitization actions. Dual authorization may also be known as two-person control.

Related Controls: AC-3, MP-2.

~~(7)~~(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~~, or devices~~*] either remotely or under the following conditions: [*Assignment: organization-defined conditions*].

Supplemental Guidance: This control enhancement protects data/information on organizational systems and system components~~, or devices (e.g., mobile devices)~~ if such systems or components~~, or devices~~ are obtained by unauthorized individuals. Remote purge/wipe commands require strong authentication to mitigate the risk of unauthorized individuals purging/wiping the system/component/device. The purge or wipe function can be implemented in a variety of ways including, for example, by overwriting data/information multiple times or by destroying the key necessary to decrypt encrypted data.

Related Controls: None.

(9) MEDIA SANITIZATION | DESTRUCTION OF PERSONALLY IDENTIFIABLE INFORMATION

Facilitate the destruction of personally identifiable information by:

(a) De-identifying the personally identifiable information;

(b) Proactively reviewing media to actively find personally identifiable information and removing such information; and

(c) Reviewing media as it is being archived or disposed to find and remove personally identifiable information.

Supplemental Guidance: Disposal or destruction of media containing personally identifiable information applies to originals, copies, and archived records, including system logs that may contain such information. De-identification is the general term for any process of removing the association between a set of identifying data and the data subject and is accomplished in a manner that prevents loss, theft, misuse, or unauthorized access.

Related Controls: SI-20.

References: FIPS Publication 199; NIST Special Publications 800-60-1, 800-60-2, 800-88, 800-124; NIST Interagency Report 8023.

MP-7 MEDIA USE

Control:

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 security safeguards*]; and

b. Prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner.

Supplemental Guidance: System media includes digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external or removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. This control also applies to mobile devices with information storage capability~~ (e.g., smart phones, tablets, E-readers).~~ In contrast to MP-2, which restricts user access to media, this control restricts the use of certain types of media on systems, for example, restricting/prohibiting the use of flash drives or external hard disk drives. Organizations can employ technical and

nontechnical safeguards ~~(e.g., policies, procedures, rules of behavior)~~ to restrict the use of system media. Organizations may restrict the use of portable storage devices, for example, by using physical cages on workstations to prohibit access to certain external ports, or disabling or removing the ability to insert, read or write to such devices. Organizations may also limit the use of portable storage devices to only approved devices including, for example, devices provided by the organization, devices provided by other approved organizations, and devices that are not personally owned. Finally, organizations may restrict the use of portable storage devices based on the type of device, for example, prohibiting the use of writeable, portable storage devices, and implementing this restriction by disabling or removing the capability to write to such devices. Requiring identifiable owners for portable storage devices reduces the risk of using such devices by allowing organizations to assign responsibility for addressing known vulnerabilities in the devices.

Related Controls: AC-19, AC-20, PL-4, PM-12, SC-34, SC-41.

Control Enhancements:

(1) MEDIA USE | PROHIBIT USE WITHOUT OWNER

~~**The organization prohibits the use of portable storage devices in organizational information systems when such devices have no identifiable owner.**~~

~~Supplemental Guidance: Requiring identifiable owners (e.g., individuals, organizations, or projects) for portable storage devices reduces the risk of using such technologies by allowing organizations to assign responsibility and accountability for addressing known vulnerabilities in the devices (e.g., malicious code insertion). Related control: PL-4.~~

[Withdrawn: Incorporated into MP-7].

(2) MEDIA USE | PROHIBIT USE OF SANITIZATION-RESISTANT MEDIA

Prohibit the use of sanitization-resistant media in organizational systems.

Supplemental Guidance: Sanitization-resistance refers to non-destructive sanitization techniques and applies to the capability to purge information from media. Certain types of media do not support sanitize commands, or if supported, the interfaces are not supported in a standardized way across these devices. Sanitization-resistant media include, for example, compact flash, embedded flash on boards and devices, solid state drives, and USB removable media.

Related Controls: MP-6.

References: FIPS Publication 199; NIST Special Publication 800-111.

MP-8 MEDIA DOWNGRADING

Control:

a. Establish [*Assignment: organization-defined system media downgrading process*] that includes employing downgrading mechanisms with ~~[*Assignment: organization-defined*~~ 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.

Supplemental Guidance: This control applies to all system media, digital and non-digital, subject to release outside of the organization, whether the media is considered removable or not removeable. The downgrading process, when applied to system media, 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 of media~~It also ensures that empty space on the media ~~(e.g., slack~~

~~space within files)~~ is devoid of information.

Control Enhancements:

(1) MEDIA DOWNGRADING | DOCUMENTATION OF PROCESS

Document system media downgrading actions.

Supplemental Guidance: 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.

Related Controls: None.

(2) MEDIA DOWNGRADING | EQUIPMENT TESTING

~~The organization employs [*Assignment: organization-defined tests*] of~~Test downgrading equipment and procedures ~~to verify correct performance [*Assignment: organization-defined frequency*].~~] to verify that intended downgrading actions are being achieved.

Supplemental Guidance: None.

Related Controls: None.

(3) MEDIA DOWNGRADING | CONTROLLED UNCLASSIFIED INFORMATION

Downgrade system media containing [*Assignment: organization-defined Controlled Unclassified Information (CUI)*] prior to public release ~~in accordance with applicable federal and organizational standards and policies~~.

Supplemental Guidance: None.

Related Controls: None.

(4) MEDIA DOWNGRADING | CLASSIFIED INFORMATION

Downgrade system media containing classified information prior to release to individuals without required access authorizations ~~in accordance with NSA standards and policies~~.

Supplemental Guidance: Downgrading of classified information uses approved sanitization tools, techniques, and procedures to transfer information confirmed to be unclassified from classified systems to unclassified media.

Related Controls: None.

References: None.

3.12 PRIVACY AUTHORIZATION

Quick link to Privacy Authorization summary table

PA-1 PRIVACY AUTHORIZATION POLICY AND PROCEDURES

Control:

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

1. A privacy authorization 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 privacy authorization policy and associated privacy authorization controls;

b. Designate an [*Assignment: organization-defined senior management official*] to manage the privacy authorization policy and procedures;

c. Review and update the current privacy authorization:

1. Policy [*Assignment: organization-defined frequency*]; and

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

d. Ensure that the privacy authorization procedures effectively implement the privacy authorization policy and controls; and

e. Develop, document, and implement remediation actions for violations of the privacy authorization policy.

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of the controls and control enhancements in the PA family. The risk management strategy is an important factor in establishing policy and procedures. Comprehensive policy and procedures help provide security and privacy assurance. Security and privacy program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general security and privacy policy or can be represented by multiple policies reflecting the complex nature of organizations. The procedures can be established for security and privacy programs and for systems, if needed. Procedures describe how policies or controls are implemented and can be directed at the personnel 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. It is important to recognize that restating controls does not constitute an organizational policy or procedure.

Related Controls: PA-2, PM-9, PS-8, SI-12.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-30, 800-39, 800-100.

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of the controls and control enhancements in the PA family. The risk management strategy is an important factor in establishing policy and procedures. Comprehensive policy and procedures help provide security and privacy assurance. Security and privacy program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general security and privacy policy or can be represented by multiple policies reflecting the complex nature of organizations.

The procedures can be established for security and privacy programs and for systems, if needed. Procedures describe how policies or controls are implemented and can be directed at the personnel 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. It is important to recognize that restating controls does not constitute an organizational policy or procedure.

Related Controls: PA-2, PM-9, PS-8, SI-12.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-30, 800-39, 800-100.

PA-2 AUTHORITY TO COLLECT

Control: Determine and document the legal authority that permits the collection, use, maintenance, and sharing of personally identifiable information, either generally or in support of a specific program or system need.

Supplemental Guidance: Prior to collecting personally identifiable information, organizations determine whether the collection of such information is legally authorized. Organizational officials consult with the Senior Agency Official for Privacy and legal counsel regarding the authority of any program or activity to collect personally identifiable information. The authority to collect personally identifiable information is documented in the System of Records Notice and/or Privacy Impact Assessment or other applicable documentation such as Privacy Act Statements or Computer Matching Agreements.

Related Controls: IP-4, IP-6, PA-1, PA-3, PM-9, PM-20, PM-25, RA-8, SI-12.

Control Enhancements: None.

References: None.

PA-3 PURPOSE SPECIFICATION

Control: Identify and document the purpose(s) for which personally identifiable information is collected, used, maintained, and shared in its privacy notices.

Supplemental Guidance: Statutory language often expressly authorizes specific collections and uses of personally identifiable information. When statutory language is written broadly and thus subject to interpretation, organizations consult with the Senior Agency Official for Privacy and legal counsel to verify that there is a close nexus between the general authorization and any specific collection of personally identifiable information. Once the specific purpose has been identified, the purpose is clearly described in the related privacy compliance documentation, including, for example, Privacy Impact Assessments, System of Records Notices, and Privacy Act Statements provided at the time of collection including, for example, on forms organizations use to collect personally identifiable information. Further, in order to avoid unauthorized collections or uses of personally identifiable information, personnel who manage such information receive role-based training as specified in AT-3.

Related Controls: IP-4, IP-5, IP-6, PA-2, PA-4, PM-9, PM-20, PM-26, RA-8, SC-43, SI-12.

Control Enhancements:

(1) PURPOSE SPECIFICATION | USAGE RESTRICTIONS OF PERSONALLY IDENTIFIABLE INFORMATION

Restrict the use of personally identifiable information to only the authorized purpose(s) consistent with applicable laws or regulations and/or in public notices.

Supplemental Guidance: Organizations take steps to help ensure that personally identifiable information is used only for legally authorized purposes and in a manner, compatible with the uses identified in the Privacy Act and/or in public notices. These steps include, for example, monitoring and auditing organizational use of personally identifiable information and training organizational personnel on the authorized uses of such information. With guidance from the Senior Agency Official for Privacy and where appropriate, legal counsel, organizations

document the processes and procedures for evaluating the proposed new uses of personally identifiable information to assess whether such uses fall within the scope of the organizational authorities. Where appropriate, organizations obtain consent from individuals for the new uses of personally identifiable information.

Related Controls: None.

(2) PURPOSE SPECIFICATION | AUTOMATION

Employ automated mechanisms to support records management of authorizing policies and procedures for personally identifiable information.

Supplemental Guidance: Automated mechanisms may be used to support records management of authorizing policies and procedures for personally identifiable information. Automated mechanisms augment verification that organizational policies and procedures are enforced for the management and tracking of personally identifiable information within an organization's systems.

Related Controls: CA-6, CM-12, IP-5, PM-29, PM-23, SC-16, SC-43, SI-12, SI-10, SI-15, SI-20, SI-19.

References: None.

PA-4 INFORMATION SHARING WITH EXTERNAL PARTIES

a. Develop, document, and disseminate guidelines to [*Assignment: organization-defined personnel or roles*] for the sharing of personally identifiable information externally, only for the authorized purposes identified in the Privacy Act and/or described in its notices, or for a purpose that is compatible with those purposes;

b. Evaluate proposed new instances of sharing personally identifiable information with external parties to assess whether:

1. The sharing is authorized; and

2. Additional or new public notice is required;

c. Enter into information sharing agreements with external parties that specifically:

1. Describe the personally identifiable information covered;

2. Enumerate the purpose(s) for which the personally identifiable information may be used; and

3. Include security requirements consistent with the information being shared; and

d. Monitor and audit the authorized sharing of personally identifiable information with external parties.

Supplemental Guidance: The Senior Agency Official for Privacy and where appropriate, legal counsel, review and approve proposed external sharing of personally identifiable information, including with other public, international, or private sector entities, for consistency with the uses described in the existing organizational public notice(s). Formal agreements for information sharing include, for example, Memoranda of Understanding, Letters of Intent, Memoranda of Agreement, and Computer Matching Agreements. When a proposed new instance of external sharing of personally identifiable information is not currently authorized by the Privacy Act and/or specified in a notice, organizations evaluate whether the proposed external sharing is compatible with the purpose(s) specified in the notice. If the proposed sharing is compatible, organizations review, update, and republish the Privacy Impact Assessments, System of Records Notices, website privacy policies, and other public notices, if any, to include specific descriptions of the new use(s) and obtain consent where appropriate and feasible.

Related Controls: IP-4, PM-25.

Control Enhancements: None.

References: None.

3.13 PHYSICAL AND ENVIRONMENTAL PROTECTION

Quick link to Physical and Environmental Protection summary table

PE-1 PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES

Control:

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

1. A 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 senior management official*] to manage the physical and environmental protection policy and procedures;

~~b.~~c. Review and update the current physical and environmental protection:

1. Policy [*Assignment: organization-defined frequency*]; and

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

d. Ensure that the physical and environmental protection procedures implement the physical and environmental protection policy and controls; and

e. Develop, document, and implement remediation actions for violations of the physical and environmental protection policy.

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of ~~selected security~~ the controls and control enhancements in the PE family. The risk management strategy is an important factor in establishing policy and procedures. Comprehensive policy and procedures help provide security and privacy assurance. Security and privacy program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general security and privacy policy or can be represented by multiple policies reflecting the complex nature of ~~certain~~ organizations. The procedures can be established for security and privacy programs and for ~~particular~~ systems, if needed. Procedures describe how policies or controls are implemented and can be directed at the personnel 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. It is important to recognize that restating controls does not constitute an organizational policy or procedure.

Related Controls: AT-3, PM-9, PS-8, SI-12.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-30, 800-39, 800-100.

PE-2 PHYSICAL ACCESS AUTHORIZATIONS

Control:

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.

Supplemental Guidance: This control applies to ~~organizational~~ employees and visitors. Individuals ~~(e.g., employees, contractors, and others)~~ with permanent physical access authorization credentials are not considered visitors. Authorization credentials include, for example, badges, identification cards, and smart cards. Organizations determine the strength of authorization credentials needed ~~(including level of forge-proof badges, smart cards, or identification cards)~~ consistent with ~~federal~~ applicable laws, Executive Orders, directives, regulations, policies, standards, ~~policies,~~ and ~~procedures~~guidelines. This control only applies to areas within facilities that have not been designated as publicly accessible.

Related Controls: 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.

Control Enhancements:

(1) PHYSICAL ACCESS AUTHORIZATIONS | ACCESS BY POSITION OR ROLE

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

Supplemental Guidance: None.

Related Controls: AC-2, AC-3, AC-6.

(2) PHYSICAL ACCESS AUTHORIZATIONS | TWO FORMS OF IDENTIFICATION

Require two forms of identification from [*Assignment: organization-defined list of acceptable forms of identification*] for visitor access to the facility where the system resides.

Supplemental Guidance: Acceptable forms of ~~government photo~~ identification include, for example, passports, Personal Identity Verification (PIV) cards, and drivers' licenses. For gaining access to facilities using automated mechanisms, organizations may use PIV cards, key cards, PINs, and biometrics.

Related Controls: IA-2, IA-4, IA-5.

(3) PHYSICAL ACCESS AUTHORIZATIONS | RESTRICT UNESCORTED ACCESS

Restrict unescorted access to the facility where the system resides to personnel with [*Selection (one or more): security clearances for all information contained within the system; formal access authorizations for all information contained within the system; need for access to all information contained within the system;* [*Assignment: organization-defined credentials*]].

Supplemental Guidance: Due to the highly sensitive nature of classified information stored within certain facilities, it is important that individuals lacking sufficient security clearances, access approvals, or need to know, be escorted by individuals with appropriate credentials to ensure that such information is not exposed or otherwise compromised.

Related Controls: PS-2, PS-6.

References: FIPS Publication 201; NIST Special Publications 800-76, 800-73, 800-78.

PE-3 PHYSICAL ACCESS CONTROL

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/exit points*];

c. Provide [*Assignment: organization-defined security safeguards*] to control access to areas within the facility designated as publicly accessible;

d. Escort visitors and monitor visitor activity [*Assignment: organization-defined circumstances requiring visitor escorts and monitoring*];

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 individuals are transferred or terminated.

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

Related Controls: 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-7, RA-3, SA-19, SC-28, SI-4.

Control Enhancements:

(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*].

Supplemental Guidance: This control enhancement provides additional physical security for those areas within facilities where there is a concentration of ~~(e.g., server rooms, media storage areas, data and communications centers~~system components.

Related Controls: PS-2.

(2) PHYSICAL ACCESS CONTROL | FACILITY AND SYSTEM BOUNDARIES

Perform security checks [*Assignment: organization-defined frequency*] at the physical boundary of the facility or system for exfiltration of information or removal of system components.

Supplemental Guidance: Organizations determine the extent, frequency, and/or randomness of security checks to adequately mitigate risk associated with exfiltration.

Related Controls: AC-4, SC-7.

(3) PHYSICAL ACCESS CONTROL | CONTINUOUS GUARDS ~~/ *ALARMS / MONITORING*~~

Employ guards to control [Assignment: organization ~~and/or alarms to monitor every~~-defined physical access points] to the facility where the system resides 24 hours per day, 7 days per week.

Supplemental Guidance: None.

Related Controls: CP-6, CP-7, PE-6.

(4) PHYSICAL ACCESS CONTROL | LOCKABLE CASINGS

Use lockable physical casings to protect [*Assignment: organization-defined system components*] from unauthorized physical access.

Supplemental Guidance: None.

Related Controls: None.

(5) PHYSICAL ACCESS CONTROL | TAMPER PROTECTION

Employ [*Assignment: organization-defined security safeguards*] to [*Selection (one or more): detect; prevent*] physical tampering or alteration of [*Assignment: organization-defined hardware components*] within the system.

Supplemental Guidance: Organizations implement tamper detection and prevention at selected hardware components or tamper detection at some components and tamper prevention at other components. ~~Tamper~~Such detection and prevention activities can employ many types of anti-tamper technologies including, for example, tamper-detection seals and anti-tamper coatings. Anti-tamper programs help to detect hardware alterations through counterfeiting and other supply chain-related risks.

Related Controls: SA-12, SA-16, SA-18.

(6) PHYSICAL ACCESS CONTROL | FACILITY PENETRATION TESTING

~~**The organization employs a penetration testing process that includes [*Assignment: organization-defined frequency*], unannounced attempts to bypass or circumvent security controls associated with physical access points to the facility.**~~

[Withdrawn: Incorporated into CA-8].

(7) PHYSICAL ACCESS CONTROL | PHYSICAL BARRIERS

Limit access using physical barriers.

Supplemental Guidance: Physical barriers include, for example, bollards, concrete slabs, jersey walls, and hydraulic active vehicle barriers.

Related Controls: None.

References: FIPS Publication 201; NIST Special Publications 800-73, 800-76, 800-78, 800-116.

PE-4 ACCESS CONTROL FOR TRANSMISSION ~~MEDIUM~~

Control: ~~The organization controls~~Control physical access to [*Assignment: organization-defined ~~information~~ system distribution and transmission lines*] within organizational facilities using [*Assignment: organization-defined security safeguards*].

Supplemental Guidance: ~~Physical~~ Security safeguards applied to system distribution and transmission lines prevent accidental damage, disruption, and physical tampering. Such safeguards may also be necessary to help prevent eavesdropping or modification of unencrypted transmissions. ~~Security safeguards~~Safeguards used to control physical access to system distribution and transmission lines include, for example, locked wiring closets; disconnected or locked spare jacks; protection of cabling by conduit or cable trays; and wiretapping sensors.

Related Controls: AT-3, IA-4, MP-2, MP-4, PE-2, PE-3, PE-5, PE-9, SC-7, SC-8.

Control Enhancements: None.

References: None.

PE-5 ACCESS CONTROL FOR OUTPUT DEVICES

Control: Control physical access to ~~information system~~output from [*Assignment: organization-defined output devices*] to prevent unauthorized individuals from obtaining the output.

Supplemental Guidance: Controlling physical access to output devices includes, for example, placing output devices in locked rooms or other secured areas and allowing access to authorized individuals only; placing output devices in locations that can be monitored by organizational personnel~~.~~; installing monitor or screen filters; and using headphones. Output devices include, for example, monitors, printers, copiers, scanners, facsimile machines, and audio devices.

Related Controls: PE-2, PE-3, PE-4, PE-18.

Control Enhancements:

(1) ACCESS CONTROL FOR OUTPUT DEVICES | ACCESS TO OUTPUT BY AUTHORIZED INDIVIDUALS

~~**Controls physical access to output from [*Assignment: organization-defined output devices*]; and Ensures**~~**Verify that only authorized individuals receive output from ~~the device~~output devices.**

Supplemental Guidance: ~~Controlling physical access to selected~~ Methods to ensure only authorized individuals receive output from output devices include, for example, placing printers, copiers, and facsimile machines in controlled areas with keypad or card reader access controls; and limiting access to individuals with certain types of badges.

Related Controls: None.

(2) ACCESS CONTROL FOR OUTPUT DEVICES | ACCESS TO OUTPUT BY INDIVIDUAL IDENTITY

~~**The information system:**~~

~~**Controls physical access to**~~ **Link individual identity to receipt of output from ~~[*Assignment: organization-defined*~~ output devices~~]; and~~.**

~~**Links**~~

~~**(a)**~~ Supplemental Guidance: Methods to link individual identity to receipt of ~~the~~ output from ~~the device.~~

~~Controlling physical access to selected~~ output devices include, for example, installing security functionality on ~~printers, copiers, and~~ facsimile machines ~~that~~, copiers, and printers. Such functionality allows organizations to implement authentication ~~(e.g., using a PIN or hardware token)~~ on output devices prior to the release of output to individuals.

Related Controls: None.

(3) ACCESS CONTROL FOR OUTPUT DEVICES | MARKING OUTPUT DEVICES

Mark [*Assignment: organization-defined system output devices*] indicating the appropriate security marking of the information permitted to be output from the device.

Supplemental Guidance: Outputs devices include, for example, printers, monitors, facsimile machines, scanners, copiers, and audio devices. ~~This control enhancement is generally applicable to information system output devices other than mobiles devices.~~

Related Controls: None.

References: NIST Interagency Report 8023.

PE-6 MONITORING PHYSICAL ACCESS

Control:

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.

Supplemental Guidance: Monitoring of physical access includes publicly accessible areas within organizational facilities. This can be accomplished for example, by the employment of guards; the use of video surveillance equipment such as cameras; or the use of sensor devices. Organizational incident response capabilities include investigations of and responses to detected physical security incidents. Security incidents include, for example, ~~apparent~~ security violations or suspicious physical access activities. Suspicious physical access activities include, for example, accesses outside of normal work hours; repeated accesses to areas not normally accessed; accesses for unusual lengths of time; and out-of-sequence accesses.

Related Controls: AU-6, AU-9, CA-7, CP-10, IR-4, IR-8.

Control Enhancements:

(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.

Supplemental Guidance: None.

Related Controls: None.

(2) MONITORING PHYSICAL ACCESS | AUTOMATED INTRUSION RECOGNITION AND RESPONSES

Employ automated mechanisms to recognize [*Assignment: organization-defined classes or types of intrusions*] and initiate [*Assignment: organization-defined response actions*].

Supplemental Guidance: None.

Related Controls: SI-4.

(3) MONITORING PHYSICAL ACCESS | VIDEO SURVEILLANCE

Employ video surveillance of [*Assignment: organization-defined operational areas*] and retain video recordings for [*Assignment: organization-defined time-period*].

Supplemental Guidance: This control enhancement focuses on recording surveillance video for purposes of subsequent review, if circumstances so warrant ~~(e.g., a break in detected by other means).~~ It does not require monitoring surveillance video although organizations may choose to do so. Note that there may be legal considerations when performing and retaining video surveillance, especially if such surveillance is in a public location.

Related Controls: None.

(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*].

Supplemental Guidance: This control enhancement provides additional monitoring for those areas within facilities where there is a concentration of system components including, for example, server rooms, media storage areas, and communications centers.

Related Controls: None.

References: None.

PE-7 VISITOR CONTROL

[Withdrawn: Incorporated into PE-2 and PE-3].

PE-8 VISITOR ACCESS RECORDS

Control:

a. Maintain visitor access records to the facility where the system resides for [*Assignment: organization-defined time-period*]; and

b. Review visitor access records [*Assignment: organization-defined frequency*].

Supplemental Guidance: Visitor access records include, for example, names and organizations of persons visiting; visitor signatures; forms of identification; dates of access; entry and departure times; purpose of visits; and names and organizations of persons visited. ~~Visitor~~ Access records are not required for publicly accessible areas.

Control Enhancements:

(1) VISITOR ACCESS RECORDS | AUTOMATED RECORDS MAINTENANCE AND REVIEW

Employ automated mechanisms to facilitate the maintenance and review of visitor access records.

Supplemental Guidance: None.

Related Controls: None.

(2) VISITOR ACCESS RECORDS | PHYSICAL ACCESS RECORDS

[Withdrawn: Incorporated into PE-2].

References: None.

PE-9 POWER EQUIPMENT AND CABLING

Control: Protect power equipment and power cabling for the system from damage and destruction.

Supplemental Guidance: Organizations determine the types of protection necessary for the power equipment and cabling employed at different locations both internal and external to organizational facilities and environments of operation. This includes, for example, generators and power cabling outside of buildings; internal cabling and uninterruptable power sources within an office or data center; and power sources for self-contained entities such as vehicles and satellites.

Related Controls: PE-4.

Control Enhancements:

(1) POWER EQUIPMENT AND CABLING | REDUNDANT CABLING

Employ redundant power cabling paths that are physically separated by [*Assignment: organization-defined distance*].

Supplemental Guidance: Physically separate and redundant power cables ensure that power continues to flow in the event one of the cables is cut or otherwise damaged.

Related Controls: None.

(2) POWER EQUIPMENT AND CABLING | AUTOMATIC VOLTAGE CONTROLS

Employ automatic voltage controls for [*Assignment: organization-defined critical system components*].

Supplemental Guidance: Automatic voltage controls can monitor and control voltage. Such controls include, for example, voltage regulators, voltage conditioners, and voltage stabilizers.

Related Controls: None.

References: None.

PE-10 EMERGENCY SHUTOFF

Control:

a. Provide the capability of shutting off power to the 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 safe and easy access for personnel; and

c. Protect emergency power shutoff capability from unauthorized activation.

Supplemental Guidance: This control applies primarily to facilities containing concentrations of system resources including, for example, data centers, server rooms, rooms/buildings containing computer-controlled machinery, and mainframe computer rooms.

Related Controls: PE-15.

Control Enhancements:

(1) EMERGENCY SHUTOFF | ACCIDENTAL AND UNAUTHORIZED ACTIVATION

[Withdrawn: Incorporated into PE-10].

References: None.

PE-11 EMERGENCY POWER

Control: Provide a short-term uninterruptible power supply to facilitate [*Selection (one or more): an orderly shutdown of the system; transition of the system to long-term alternate power*] in the event of a primary power source loss.

Supplemental Guidance: None.

Related Controls: AT-3, CP-2, CP-7.

Control Enhancements:

(1) EMERGENCY POWER | LONG-TERM ALTERNATE POWER SUPPLY — MINIMAL OPERATIONAL CAPABILITY

Provide a long-term alternate power supply for the system that can maintain minimally required operational capability in the event of an extended loss of the primary power source.

Supplemental Guidance: This control enhancement can be satisfied, for example, by using a secondary commercial power supply or other external power supply. The long-term alternate power supplies for organizational systems are either manually or automatically activated.

Related Controls: None.

(2) EMERGENCY POWER | LONG-TERM ALTERNATE POWER SUPPLY — SELF-CONTAINED

Provide a long-term alternate power supply for the system 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.

Supplemental Guidance: This control enhancement can be satisfied, for example, by using one or more generators with sufficient capacity to meet the needs of the organization. Long-term alternate power supplies for organizational systems are either manually or automatically activated.

Related Controls: None.

References: None.

PE-12 EMERGENCY LIGHTING

Control: Employ and maintain automatic emergency lighting for the system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

Supplemental Guidance: This control applies primarily to facilities containing concentrations of system resources including, for example, data centers, server rooms, and mainframe computer rooms.

Related Controls: CP-2, CP-7.

Control Enhancements:

(1) EMERGENCY LIGHTING | ESSENTIAL MISSIONS AND BUSINESS FUNCTIONS

Provide emergency lighting for all areas within the facility supporting essential missions and business functions.

Supplemental Guidance: None.

Related Controls: None.

References: None.

PE-13 FIRE PROTECTION

Control: Employ and maintain fire suppression and detection devices/systems for the system that are supported by an independent energy source.

Supplemental Guidance: This control applies primarily to facilities containing concentrations of system resources including, for example, data centers, server rooms, and mainframe computer rooms. Fire suppression and detection devices or systems that may require an independent energy source include, for example, sprinkler systems~~, handheld fire extinguishers~~, fixed fire hoses, and smoke detectors.

Related Controls: AT-3.

Control Enhancements:

(1) FIRE PROTECTION | DETECTION DEVICES AND SYSTEMS

Employ fire detection devices/systems for the system that activate automatically and notify [*Assignment: organization-defined personnel or roles*] and [*Assignment: organization-defined emergency responders*] in the event of a fire.

Supplemental Guidance: Organizations can identify specific personnel, roles, and emergency responders if individuals on the notification list need to have appropriate access authorizations and/or clearances, for example, to obtain access to facilities where classified operations are taking place or where there are systems containing classified information.

Related Controls: None.

(2) FIRE PROTECTION | AUTOMATIC SUPPRESSION DEVICES AND SYSTEMS

(a) Employ fire suppression devices/systems for the system that provide automatic notification of any activation to [*Assignment: organization-defined personnel or roles*] and [*Assignment: organization-defined* emergency responders]; and

(b) Employ an automatic fire suppression capability for the system when the facility is not staffed on a continuous basis.

Supplemental Guidance: Organizations can identify specific personnel, roles, and emergency responders if individuals on the notification list need to have appropriate access authorizations and/or clearances, for example, to obtain access to facilities where classified operations are taking place or where there are systems containing classified information.

Related Controls: None.

(3) FIRE PROTECTION | AUTOMATIC FIRE SUPPRESSION

~~**The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.**~~

[Withdrawn: Incorporated into PE-13(2)].

(4) FIRE PROTECTION | INSPECTIONS

Verify that the facility undergoes [*Assignment: organization-defined frequency*] fire protection inspections by authorized and qualified inspectors and resolves identified deficiencies within [*Assignment: organization-defined time-period*].

Supplemental Guidance: None.

Related Controls: None.

References: None.

PE-14 TEMPERATURE AND HUMIDITY CONTROLS

Control:

a. Maintain temperature and humidity levels within the facility where the system resides at [*Assignment: organization-defined acceptable levels*]; and

b. Monitor temperature and humidity levels [*Assignment: organization-defined frequency*].

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

Related Controls: AT-3, CP-2.

Control Enhancements:

(1) TEMPERATURE AND HUMIDITY CONTROLS | AUTOMATIC CONTROLS

Employs automatic temperature and humidity controls in the facility to prevent fluctuations potentially harmful to the system.

Supplemental Guidance: None.

Related Controls: None.

(2) TEMPERATURE AND HUMIDITY CONTROLS | MONITORING WITH ALARMS AND NOTIFICATIONS

Employ temperature and humidity monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment to [*Assignment: organization-defined personnel or roles*].

Supplemental Guidance: None.

Related Controls: None.

References: None.

PE-15 WATER DAMAGE PROTECTION

Control: Protect the system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

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

Related Controls: AT-3, PE-10.

Control Enhancements:

(1) WATER DAMAGE PROTECTION | AUTOMATION SUPPORT

Employ automated mechanisms to detect the presence of water near the system and alert [*Assignment: organization-defined personnel or roles*].

Supplemental Guidance: Automated mechanisms include, for example, water detection sensors, alarms, and notification systems.

Related Controls: None.

References: None.

PE-16 DELIVERY AND REMOVAL

Control: Authorize, monitor, and control [*Assignment: organization-defined types of system components*] entering and exiting the facility and maintain records of those items.

Supplemental Guidance: ~~Effectively~~ Enforcing authorizations for entry and exit of system components may require restricting access to delivery areas and ~~possibly~~ isolating the areas from the system and media libraries.

Related Controls: CM-3, MA-2, MA-3, MP-5, SA-12.

Control Enhancements: None.

References: None.

PE-17 ALTERNATE WORK SITE

Control:

a. Determine and document the [*Assignment: organization-defined alternate work sites*] allowed for use by employees;

~~a.~~b. Employ [*Assignment: organization-defined security and privacy controls*] at alternate work sites;

~~b.~~c. Assess~~es as feasible,~~ the effectiveness of security and privacy controls at alternate work sites; and

~~c.~~d. Provide a means for employees to communicate with information security and privacy personnel in case of security or privacy incidents or problems.

Supplemental Guidance: Alternate work sites include, for example, government facilities or private residences of employees. While distinct from alternative processing sites, alternate work sites can

provide readily available alternate locations during contingency operations. Organizations can define different sets of controls for specific alternate work sites or types of sites depending on the work-related activities conducted at those sites. This control supports the contingency planning activities of organizations ~~and the federal telework initiative.~~ .

Related Controls: AC-17, AC-18, CP-7.

Control Enhancements: None.

References: NIST Special Publication 800-46.

PE-18 LOCATION OF SYSTEM COMPONENTS

Control: Position system components within the facility to minimize potential damage from [*Assignment: organization-defined physical and environmental hazards*] and to minimize the opportunity for unauthorized access.

Supplemental Guidance: Physical and environmental hazards include, for example, flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electromagnetic pulse, electrical interference, and other forms of incoming electromagnetic radiation. Organizations also consider the location of ~~physical~~ entry points where unauthorized individuals, while not being granted access, might nonetheless be ~~in close~~near systems. Such proximity can increase the ~~potential for~~risk of unauthorized access to organizational communications ~~(e.g., through the use of~~, including, for example, using wireless sniffers or microphones.

Related Controls: CP-2, PE-5, PE-19, PE-20, RA-3.

Control Enhancements:

(1) LOCATION OF SYSTEM COMPONENTS | FACILITY SITE

(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.

Supplemental Guidance: None.

Related Controls: PM-8.

References: None.

PE-19 INFORMATION LEAKAGE

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

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

Related Controls: AC-18, PE-18, PE-20.

Control Enhancements:

(1) INFORMATION LEAKAGE | NATIONAL EMISSIONS AND TEMPEST POLICIES AND PROCEDURES

Protect system components, associated data communications, and networks in accordance with national Emissions ~~and TEMPEST~~Security policies and procedures based on the security category or classification of the information.

Supplemental Guidance: Emissions Security (EMSEC) policies include the former TEMPEST policies.

Related Controls: None.

References: FIPS Publication 199.

PE-20 ASSET MONITORING AND TRACKING

Control: Employ [*Assignment: organization-defined asset location technologies*] to track and monitor the location and movement of [*Assignment: organization-defined assets*] within [*Assignment: organization-defined controlled areas*].

~~(1) Ensures that asset location technologies are employed in accordance with applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance.~~

Supplemental Guidance: Asset location technologies can help organizations ensure that critical assets, including, for example, vehicles, equipment, or essential system components remain in authorized locations. Organizations consult with the Office of the General Counsel and the Senior Agency Official for Privacy ~~(SAOP)/Chief Privacy Officer (CPO)~~ regarding the deployment and use of asset location technologies to address potential privacy concerns.

Related Controls: CM-8, PM-8.

Control Enhancements: None.

References: None.

PE-21 ELECTROMAGNETIC PULSE PROTECTION

Control: Employ [*Assignment: organization-defined security safeguards*] against electromagnetic pulse damage for [*Assignment: organization-defined systems and system components*].

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

Related Controls: PE-18, PE-19.

Control Enhancements: None.

References: None.

PE-22 COMPONENT MARKING

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

Supplemental Guidance: Hardware components that may require marking include, for example, input devices marked to indicate the classification of the network to which they are connected or a multifunction function printer or copier residing in a classified area. Security marking refers to the application or use of human-readable security attributes. Security labeling refers to the application or use of security attributes regarding internal data structures within systems. Security marking is generally not required for hardware components processing, storing, or transmitting information determined by organizations to be in the public domain or to be publicly releasable. However, organizations may require markings for hardware components processing, storing, or transmitting public information indicating that such information is publicly releasable. The marking of system hardware components reflects applicable laws, Executive Orders, directives, policies, regulations, standards, and guidelines.

Related Controls: AC-16, MP-3.

Control Enhancements: None.

References: None.

3.14 PLANNING

Quick link to Planning summary table

PL-1 ~~SECURITY~~ PLANNING POLICY AND PROCEDURES

Control:

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

1. Security and privacy planning policies that:

(a) Address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Are consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the security and privacy planning policies and the associated security and privacy planning controls;

b. Designate an [*Assignment: organization-defined senior management official*] to manage the security and privacy planning policies and procedures;

~~b.~~c. Review and update the current security and privacy planning:

1. Policies [*Assignment: organization-defined frequency*]; and

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

d. Ensure that the security and privacy planning procedures implement the security and privacy planning policies and controls; and

e. Develop, document, and implement remediation actions for violations of the planning policy.

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of ~~selected security~~the controls and control enhancements in the PL family. The risk management strategy is an important factor in establishing policy and procedures ~~reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards,~~. Comprehensive policy and ~~guidance,~~procedures help provide security and privacy assurance. Security and privacy program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general ~~information~~ security ~~policy for organizations~~and privacy policies or ~~conversely,~~ can be represented by multiple policies reflecting the complex nature of ~~certain~~ organizations. The procedures can be established for ~~the~~ security ~~program in general~~and privacy programs and for ~~particular information~~ systems, if needed. ~~The~~Procedures describe how policies or controls are implemented and can be directed at the personnel 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. It is important to recognize that restating controls does not constitute an organizational ~~risk management strategy is a key factor in establishing~~ policy ~~and procedures.~~ or procedure.

Related Controls: PM-9, PS-8, SI-12.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-18, 800-30, 800-39, 800-100.

PL-2 SECURITY AND PRIVACY PLANS

Control:

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

1. Are consistent with the organization's enterprise architecture;
2. Explicitly define the authorization boundary for the system;
3. Describe the operational context of the system in terms of missions and business processes;
4. Provide the security categorization of the system including supporting rationale;
5. Describe the operational environment for the system and relationships with or connections to other systems;
6. Provide an overview of the security and privacy requirements for the system;
7. Identify any relevant overlays, if applicable;
8. Describe the security and privacy controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and
9. Are reviewed and approved by the authorizing official or designated representative prior to plan implementation;

b. Distribute copies of the security and privacy plans and communicate subsequent changes to the plans to [*Assignment: organization-defined personnel or roles*];

c. Review the security and privacy plans [*Assignment: organization-defined frequency*];

d. Update the security and privacy plans to address changes to the system and environment of operation or problems identified during plan implementation or security and privacy control assessments; and

e. Protect the security and privacy plans from unauthorized disclosure and modification.

Supplemental Guidance: Security and privacy plans relate security and privacy requirements to a set of security and privacy controls and control enhancements. The plans describe how the security and privacy controls and control enhancements meet those security and privacy requirements, but do not provide detailed, technical descriptions of the specific design or implementation of the controls and control enhancements. Security and privacy plans contain sufficient information (including the specification of parameter values for assignment and selection statements either explicitly or by reference) to enable a design and implementation that is unambiguously compliant with the intent of the plans and subsequent determinations of risk to organizational operations and assets, individuals, other organizations, and the Nation if the plan is implemented as intended. Organizations can also apply tailoring guidance to the control baselines in Appendix D ~~and CNSS Instruction 1253~~ to develop *overlays* for community-wide use or to address specialized requirements, technologies, missions, business applications, or environments of operation ~~(e.g., DoD tactical, Federal Public Key Infrastructure, or Federal Identity, Credential, and Access Management, space operations). Appendix I provides guidance on developing overlays~~.

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, for example, design and implementation specifications where more detailed information can be obtained. This reduces the documentation ~~requirements~~ associated with security and privacy programs and maintains the security- and privacy-related information in other established management and operational areas including, for example, enterprise architecture, system development life cycle, systems engineering, and acquisition. Thus, security and privacy plans do not contain detailed contingency plan or incident response plan information but instead provide explicitly or by reference, sufficient information to define what needs to be accomplished by those plans.

Related Controls: AC-2, AC-6, AC-14, AC-17, AC-20, CA-2, CA-3, CA-7, CM-9, CP-2, IR-8, MA-4, MA-5, MP-4, MP-5, PL-7, PL-8, PM-1, PM-7, PM-8, PM-9, PM-10, PM-11, RA-3, RA-9, SA-5, SA-17, SA-22, SI-12.

Control Enhancements:

(1) ~~*SYSTEM*~~ SECURITY ~~*PLAN*~~ AND PRIVACY PLANS | CONCEPT OF OPERATIONS

[Withdrawn: Incorporated into PL-7].

(2) ~~*SYSTEM*~~ SECURITY ~~*PLAN*~~ AND PRIVACY PLANS | FUNCTIONAL ARCHITECTURE

~~[~~Withdrawn: Incorporated into PL-8].

(3) ~~*SYSTEM*~~ SECURITY AND PRIVACY PLANS | PLAN ~~| *PLAN /*~~AND COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES

Plan and coordinate security~~-~~ and privacy-related activities affecting the system with [*Assignment: organization-defined individuals or groups*] before conducting such activities to reduce the impact on other organizational entities.

Supplemental Guidance: Security- and privacy-related activities include, for example, security and privacy assessments, audits and inspections, hardware and software maintenance, patch management, and contingency plan testing. ~~Advance~~ Planning and coordination includes emergency and nonemergency (i.e., planned or non-urgent unplanned) situations. The process defined by organizations to plan and coordinate security- and privacy-related activities can be included in security and privacy plans for systems or other documents, as appropriate.

Related Controls: CP-4, IR-4.

References: NIST Special Publication 800-18.

PL-3 SYSTEM SECURITY PLAN UPDATE

[Withdrawn: Incorporated into PL-2].

PL-4 RULES OF BEHAVIOR

Control:

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 ~~signed~~ 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 signed a previous version of the rules of behavior to read and re-sign [*Selection (one or more): [Assignment: organization-defined frequency]; when the rules ~~of behavior~~ are revised or updated*.]

Supplemental Guidance: This control enhancement applies to organizational users. Organizations consider rules of behavior based on individual user roles and responsibilities, differentiating, for example, between rules that apply to privileged users and rules that apply to the general user population. Establishing rules of behavior for some types of non-organizational users including, for example, individuals who simply receive data or information from federal systems, is often not feasible given the large number of such users and the limited nature of their interactions with the systems. Rules of behavior for organizational and non-organizational users can also be established in AC-8, System Use Notification. PL-4b, the ~~signed~~documented acknowledgment portion of the control, may be satisfied by the security and privacy awareness training and the role-based security and privacy training programs conducted by organizations if such training includes rules of behavior. ~~Organizations can use electronic signatures~~Documented acknowledgements for ~~acknowledging~~ rules of behavior may include, for example, electronic or physical signatures; and electronic agreement check boxes/radio buttons.

Related Controls: 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.

Control Enhancements:

(1) RULES OF BEHAVIOR | SOCIAL MEDIA AND NETWORKING RESTRICTIONS

Include in the rules of behavior, explicit restrictions on the use of social media and networking sites and posting organizational information on public websites.

Supplemental Guidance: This control enhancement addresses rules of behavior related to the use of social media and networking sites when organizational personnel are using such sites for official duties or in the conduct of official business; when organizational information is involved in social media and networking transactions; and when personnel are accessing social media and networking sites from organizational systems. Organizations also address specific rules that prevent unauthorized entities from obtaining, either directly or through inference, non-public organizational information ~~(e.g.,~~from social media and networking sites. Examples of non-public information include system account information~~,~~ and personally identifiable information.

Related Controls: None.

References: NIST Special Publication 800-18.

PL-5 PRIVACY IMPACT ASSESSMENT

[Withdrawn: Incorporated into RA-8].

PL-6 SECURITY-RELATED ACTIVITY PLANNING

[Withdrawn: Incorporated into PL-2].

PL-7 ~~SECURITY~~ CONCEPT OF OPERATIONS

Control:

a. Develop a Concept of Operations (CONOPS) for the system ~~containing at a minimum,~~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*].

Supplemental Guidance: The security and privacy CONOPS may be included in the security or privacy plans for the system or in other system development life cycle documents, as appropriate. Changes to the CONOPS are reflected in ongoing updates to the security and privacy plans, the security and privacy architectures, and other appropriate organizational documents ~~(e.g., security specifications~~, including, for example, system development life cycle documents, procurement specifications, and systems~~/security~~ engineering documents.

Related Controls: PL-2, SA-2, SI-12.

Control Enhancements: None.

References: None.

PL-8 ~~INFORMATION~~ SECURITY ~~ARCHITECTURE~~AND PRIVACY ARCHITECTURES

Control:

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

1. Describe the philosophy, requirements, and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information;

2. Describe the philosophy, requirements, and approach to be taken for processing personally identifiable information;

~~2.~~3. Describe how the security and privacy architectures are integrated into and support the enterprise architecture; and

~~3.~~4. Describe any security and privacy-related assumptions about, and dependencies on, external services;

b. Review and update the security and privacy architectures [*Assignment: organization-defined frequency*] to reflect updates in the enterprise architecture; and

c. ~~Ensures that~~Reflect planned security and privacy architecture changes ~~are reflected~~ in the security and privacy plans, the Concept of Operations (CONOPS), and organizational procurements and acquisitions.

Supplemental Guidance: This control addresses actions taken by organizations in the design and development of systems. The security and privacy architectures at the ~~individual~~ system level are consistent with and complement the ~~more global,~~ organization-wide security and privacy architectures described in PM-7 that are integral to and developed as part of the enterprise architecture. The security and privacy architectures include an architectural description, the placement and allocation of security and privacy functionality (including security and privacy controls), security- and privacy-related information for external interfaces, information being exchanged across the interfaces, and the protection mechanisms associated with each interface. In addition, the security and privacy architectures can include other ~~important security-related~~ information, for example, user roles and the access privileges assigned to each role, unique security and privacy requirements, types of information processed, stored, and transmitted by the system, restoration priorities of information and system services, and any other specific protection needs.

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 important to 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 security and privacy architectures. The development of the security and privacy architectures is coordinated with the Senior Agency Information Security Officer and the Senior Agency Official for Privacy ~~(SAOP)/Chief Privacy Officer (CPO)~~ to ensure that security and privacy controls needed to support security and privacy requirements are identified and effectively implemented. PL-8 is primarily directed at organizations ~~(i.e., internally focused) to help~~to ensure that ~~organizations~~they develop security and privacy architectures for the system, and that the architectures are integrated with or tightly coupled to the enterprise architecture through the organization-wide security and privacy architectures. In contrast, SA-17 is primarily directed at external information technology product~~/~~ and system developers and integrators ~~(although SA-17 could be used internally within organizations for in-house system development).~~ SA-17, which is complementary to PL-8, is selected when organizations outsource the development of systems or system components to external entities, and there is a need to demonstrate consistency with the organization's enterprise architecture and security and privacy architectures.

Related Controls: CM-2, CM-6, PL-2, PL-7, PL-9, PM-7, PM-29, RA-9, SA-3, SA-5, SA-8, SA-17.

Control Enhancements:

(1) ~~*INFORMATION*~~ SECURITY ~~*ARCHITECTURE*~~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 security and privacy safeguards*] to [*Assignment: organization-defined locations and architectural layers*]; and

(b) Ensures that the allocated security and privacy safeguards operate in a coordinated and mutually reinforcing manner.

Supplemental Guidance: Organizations strategically allocate security safeguards (procedural, technical, or both) in the security architecture so that adversaries must overcome multiple safeguards to achieve their objective. Requiring adversaries to defeat multiple mechanisms makes it more difficult to successfully attack critical information resources ~~(i.e., increases adversary~~ by increasing the work factor~~) and~~ of the adversary. It also increases the likelihood

of detection. The coordination of allocated safeguards is essential to ensure that an attack that involves one safeguard does not create adverse unintended consequences ~~(e.g.,~~by interfering with other safeguards. Examples of such unintended consequences include system lockout~~,~~ and cascading alarms~~) by interfering with another safeguard.~~. Placement of security safeguards is ~~a key~~an important activity~~. Greater asset~~ requiring thoughtful analysis. The criticality or ~~information~~ value ~~merits~~of the organizational asset is a key consideration in providing additional layering. ~~Thus, an organization may choose to place anti-virus software at organizational boundary layers, email/web servers, notebook computers, and workstations to maximize the number of related safeguards adversaries must penetrate before compromising the information and information systems~~

Related Controls: SC-29, SC-36.

(2) SECURITY ~~*ARCHITECTURE*~~AND PRIVACY ARCHITECTURES | SUPPLIER DIVERSITY

Require that [*Assignment: organization-defined security and privacy safeguards*] allocated to [*Assignment: organization-defined locations and architectural layers*] are obtained from different suppliers.

Supplemental Guidance: Different information technology products have different strengths and weaknesses. Providing a broad spectrum of products complements the individual offerings. For example, vendors offering malicious code protection typically update their products at different times, often developing solutions for known viruses, Trojans, or worms based on their priorities and development schedules. By having different products at different locations ~~(e.g., server, boundary, desktop)~~ there is an increased likelihood that at least one will detect the malicious code.

Related Controls: SA-12, SC-29.

References: None.

PL-9 CENTRAL MANAGEMENT

Control: Centrally manage [*Assignment: organization-defined security and privacy controls and related processes*].

Supplemental Guidance: Central management refers to the organization-wide management and implementation of selected security and privacy controls and related processes. This~~Central Management~~ includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed ~~security~~ controls and processes. As the central management of security and privacy controls is generally associated with the concept of common controls, such management promotes and facilitates standardization of control implementations and management and 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. As part of the security and privacy control selection processes, organizations determine which controls may be suitable for central management based on organizational resources and capabilities. ~~Organizations consider that it may~~ It is not always possible to centrally manage every aspect of a security or privacy 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. Those controls and control enhancements that are candidates for full or partial central management include, but are not limited to: AC-2 (1) (2) (3) (4); AC-17 (1) (2) (3) (9); AC-18 (1) (3) (4) (5); AC-19 (4); AC-22; AC-23; AT-2 (1) (2); AT-3 (1) (2) (3); AT-4; AU-6 (1) (3) (5) (6) (9); AU-7 (1) (2); AU-11, AU-13, AU-16, CA-2 (1) (2) (3); CA-3 (1) (2) (3); CA-7 (1); CA-9; CM-2 (1) (2); CM-3 (1) (4); CM-4; CM-6 (1); CM-7 (4) (5); CM-8 (all); CM-9 (1); CM-10; CM-11; CP-7 (all); CP-8 (all); SC-43; SI-2; SI-3; SI-7; and SI-8.

Related Controls: PL-8, PM-9.

Control Enhancements: None.

References: NIST Special Publication 800-37.

PL-10 BASELINE SELECTION

Control: Select a control baseline for the system.

Supplemental Guidance: The selection of an appropriate control baseline is determined by the needs of organizational stakeholders. Stakeholder needs and concerns consider mission and business requirements and mandates imposed by applicable laws, Executive Orders, directives, policies, regulations, standards, and guidelines. For example, the three control baselines in Appendix D are based on the requirements from the Federal Information Security Modernization Act (FISMA) and the Privacy Act. These requirements, along with the NIST standards and guidelines implementing the legislation, require organizations to select one of the control baselines after the reviewing the information types and the information that is processed, stored, and transmitted on organizational systems; analyzing the potential adverse impact or consequences of the loss or compromise of the system or information on the organization's operations and assets, individuals, other organizations or the Nation; and considering the results from organizational and system assessments of risk. Nonfederal organizations that are part of other communities of interest including the U.S. critical infrastructure sectors, can develop similar control baselines (using the controls in Chapter Three) that represent the needs and concerns of those entities.

Related Controls: PL-11, RA-2, RA-3, SA-8.

Control Enhancements: None.

References: FIPS Publications 199, 200; NIST Special Publications 800-30, 800-37, 800-39, 800-60-1, 800-60-2, 800-160.

PL-11 BASELINE TAILORING

Control: Tailor the selected control baseline by applying specified tailoring actions.

Supplemental Guidance: The concept of tailoring allows organizations to specialize or customize a set of baseline controls by applying a defined set of tailoring actions. These actions facilitate such specialization and customization by allowing organizations to develop security and privacy plans that reflect their specific missions and business functions, the environments where their systems operate, the threats and vulnerabilities that can affect their systems, and any other conditions or situations that can impact their mission or business success. The tailoring actions are described in Appendix G. Tailoring a control baseline is accomplished by identifying and designating common controls; applying scoping considerations; selecting compensating controls; assigning values to control parameters; supplementing the control baseline with additional controls, as needed; and providing information for control implementation. The general tailoring actions in Appendix G can be supplemented with additional actions based on the needs of organizations. Tailoring actions can be applied to the baselines in Appendix D in accordance with the security requirements from the Federal Information Security Modernization Act (FISMA) and the privacy requirements from the Privacy Act. Alternatively, other communities of interest adopting different control baselines can apply the tailoring actions in Appendix G to specialize or customize the controls that represent the specific needs and concerns of those entities.

Related Controls: PL-10, RA-2, RA-3, RA-9, SA-8, SA-12.

Control Enhancements: None.

References: FIPS Publications 199, 200; NIST Special Publications 800-30, 800-37, 800-39, 800-160.

3.15 PROGRAM MANAGEMENT

Quick link to Program Management summary table

PM-1 INFORMATION SECURITY PROGRAM PLAN

Control:

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 the organization-wide information security program plan [*Assignment: organization-defined frequency*];

c. Update the information security program plan to address organizational changes and problems identified during plan implementation or control assessments; and

d. Protect the information security program plan from unauthorized disclosure and modification.

Supplemental Guidance: Information security program plans can be represented in single documents or compilations of documents at the discretion of organizations. The plans document the program management controls and organization-defined common controls. Information security program plans provide sufficient information about the program management controls/common controls (including specification of parameters for any assignment and selection statements either explicitly or by reference) to enable implementations that are unambiguously compliant with the intent of the plans and a determination of the risk to be incurred if the plans are implemented as intended. Security plans for individual systems and the organization-wide information security program plan, provide complete coverage for all security controls employed within the organization. Common controls are documented in an appendix to the organization's information security program plan unless the controls are included in a separate security plan for a system. The organization-wide information security program plan will indicate which separate security plans contain descriptions of common controls.

Organizations have the flexibility to describe common controls in a single document or in multiple documents. For multiple documents, the documents describing common controls are included as attachments to the information security program plan. If the information security program plan contains multiple documents, the organization specifies in each document the organizational official or officials responsible for the development, implementation, assessment, authorization, and monitoring of the respective common controls. For example, the Facilities Management Office may develop, implement, assess, authorize, and continuously monitor common physical and environmental protection controls from the PE family when such controls are not associated with a particular system but instead, support multiple systems.

Related Controls: PL-2, PM-8, PM-12, RA-9, SA-12, SI-12.

Control Enhancements: None.

References: None.

PM-2 INFORMATION SECURITY PROGRAM ROLES ~~SENIOR INFORMATION SECURITY OFFICER~~

Control:

a. Appoint a Senior Agency Information Security Officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program;

b. Appoint a Senior Accountable Official for Risk Management to align information security management proceeses with strategic, operational, and budgetary planning procceses; and

c. Appoint a Risk Executive (function) to view and analyze risk from an organization-wide perspective and ensure management of risk is consistent across the organization.

Supplemental Guidance: The senior 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. The senior accountable official for risk management leads the risk executive (function) in organization-wide risk management activities.

Related Controls: None.

Control Enhancements: None.

References: NIST Special Publications 800-37, 800-39; OMB Memorandum 17-25.

PM-3 INFORMATION SECURITY AND PRIVACY RESOURCES

Control:

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. ~~Employs a business case/Exhibit 300/Exhibit 53 to record the resources required.~~ 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. ~~Ensure that information security resources are available for expenditure as planned.~~ Make available for expenditure, the planned information security and privacy resources.

Supplemental Guidance: Organizations consider establishing champions for information security and privacy efforts and as part of including the necessary resources, assign specialized expertise and resources as needed. Organizations may designate and empower an Investment Review Board or similar group to manage and provide oversight for the information security-and privacy-related aspects of the capital planning and investment control process.

Related Controls: PM-4, SA-2.

Control Enhancements: None.

References: NIST Special Publication 800-65.

PM-4 PLAN OF ACTION AND MILESTONES PROCESS

Control:

a. Implement a process to ensure that plans of action and milestones for the security and privacy programs and associated organizational systems:

   1. Are developed and maintained;

2. Document the remedial information security and privacy 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.

Supplemental Guidance: The plan of action and milestones is a key document in the information security and privacy programs and is subject to reporting requirements established by the Office of Management and Budget. Organizations view plans of action and milestones from an enterprise-wide perspective, prioritizing risk response actions and ensuring consistency with the goals and objectives of the organization. Plan of action and milestones updates are based on findings from control assessments and continuous monitoring activities. ~~OMB FISMA reporting guidance contains instructions regarding organizational plans of action and milestons.~~

Related Controls: CA-5; CA-7, PM-3, RA-7, SI-12.

Control Enhancements: None.

References: NIST Special Publications 800-37.

PM-5 SYSTEM INVENTORY

Control: Develop and maintain an inventory of organizational systems.

Supplemental Guidance: ~~This control addresses the inventory requirements in FISMA.~~ OMB provides guidance on developing systems inventories and associated reporting requirements. ~~For specific information system inventory reporting requirements, organizaitons consult OMB annual FISMA reporting guidance.~~ This control refers to an organization-wide inventory of systems, not system components as described in CM-8.

Related Controls: None.

Control Enhancements: None.

References: None.

PM-6 ~~INFORMATION SECURITY~~ MEASURES OF PERFORMANCE

Control: Develop, monitor, and report on the results of information security and privacy measures of performance.

Supplemental Guidance: Measures of performance are outcome-based metrics used by an organization to measure the effectiveness or efficiency of the information security and privacy programs and the security and privacy controls employed in support of the program.

Related Controls: CA-7.

Control Enhancements: None.

References: NIST Special Publications 800-55, 800-137.

PM-7 ENTERPRISE ARCHITECTURE

Control: Develop an enterprise architecture with consideration for information security, privacy, and the resulting risk to organizational operations and assets, individuals, other organizations, and the Nation.

Supplemental Guidance: The integration of security and privacy requirements and controls into the enterprise architecture ensures that security and privacy considerations are addressed early in the system development life cycle and are directly and explicitly related to the organization's mission and business processes. The process of security and privacy requirements integration also embeds

into the enterprise architecture, the organization's security and privacy architectures consistent with the organizational risk management and information security and privacy strategies. For PM-7, the security and privacy architectures are developed at a system-of-systems level, representing all organizational systems. For PL-8, the security and privacy architectures are developed at a level representing an individual system. The system-level architectures are consistent with the security and privacy architectures defined for the organization. Security and privacy requirements and control integration are most effectively accomplished through the rigorous application of the Risk Management Framework and supporting security standards and guidelines. ~~The Federal Segment Architecture Methodology provides guidance on integrating information security requirements and security controls into enterprise architectures.~~

Related Controls: AU-6, PL-2, PL-8, PM-11, RA-2, SA-3, SA-8, SA-17.

Control Enhancements: None.

References: NIST Special Publication 800-39.

PM-8 CRITICAL INFRASTRUCTURE PLAN

Control: Address information security and privacy issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

Supplemental Guidance: Protection strategies are based on the prioritization of critical assets and resources. The requirement and guidance for defining critical infrastructure and key resources and for preparing an associated critical infrastructure protection plan are found in applicable laws, Executive Orders, directives, policies, regulations, standards, and guidelines.

Related Controls: CP-2, CP-4, PE-18, PL-2, PM-1, PM-9, PM-11, PM-18, RA-3, SI-12.

Control Enhancements: None.

References: HSPD 7; National Infrastructure Protection Plan.

PM-9 RISK MANAGEMENT STRATEGY

Control:

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;

   2. Privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of personally identifiable information; and

   3. Supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services;

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.

Supplemental Guidance: An organization-wide risk management strategy includes, for example, an expression of the security, privacy, and supply chain risk tolerance for the organization; acceptable risk assessment methodologies; security, privacy, and supply chain risk mitigation strategies; a process for consistently evaluating security, privacy, and supply chain risk across the organization with respect to the organization's risk tolerance; and approaches for monitoring risk over time. The senior accountable official for risk management (agency head or designated official) aligns information security management proceeses with strategic, operational, and budgetary planning procceses. The use of a risk executive function, led by the senior accountable official for risk management, can facilitate consistent application of the risk management strategy organization-wide. The organization-wide risk management strategy can be informed by security, privacy, and

supply chain risk-related inputs from other sources, internal and external to the organization, to ensure the strategy is both broad-based and comprehensive.

Related Controls: All XX-1 Controls, CA-2, CA-5, CA-6, CA-7, IP-1, PA-1, PA-2, PA-3, PL-2, PM-8, PM-18, PM-31, PM-32, RA-3, RA-9, SA-4, SA-12, SC-38, SI-12.

Control Enhancements: None.

References: NIST Special Publications 800-30, 800-39, 800-161; NIST Interagency Report 8023.

PM-10 AUTHORIZATION PROCESS

Control:

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.

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

Related Controls: CA-6, CA-7, PL-2.

Control Enhancements: None.

References: NIST Special Publications 800-37, 800-39.

PM-11 MISSION AND BUSINESS PROCESS DEFINITION

Control:

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*], until achievable protection and personally identifiable information processing needs are obtained.

Supplemental Guidance: Protection needs are technology-independent, required capabilities to counter threats to organizations, individuals, systems, and the Nation through the compromise of information (i.e., loss of confidentiality, integrity, availability, or privacy). Information protection and personally identifiable information processing needs are derived from mission and business needs defined by the stakeholders in organizations, the mission and business processes defined to meet those needs, and the organizational risk management strategy. Information protection and personally identifiable information processing needs determine the required security and privacy controls for the organization and the systems supporting the mission and business processes. Inherent in defining the protection and personally identifiable information processing needs, is an understanding of adverse impact or consequences that could result if a compromise of information occurs. The categorization process is used to make such potential impact determinations. Privacy

risks to individuals can arise from the compromise of personally identifiable information, but they can also arise as unintended consequences or a byproduct of authorized processing of information at any stage of the data life cycle. Privacy risk assessments are used to prioritize the risks that are created for individuals from system processing of personally identifiable information. These risk assessments enable the selection of the required privacy controls for the organization and systems supporting the mission and business processes. Mission and business process definitions and the associated protection requirements are documented in accordance with organizational policy and procedures.

Related Controls: CP-2, PL-2, PM-7, PM-8, RA-2, SA-2.

Control Enhancements: None.

References: FIPS Publication 199; NIST Special Publication 800-60-1, 800-60-2.

PM-12 INSIDER THREAT PROGRAM

Control: Implement an insider threat program that includes a cross-discipline insider threat incident handling team.

Supplemental Guidance: Organizations handling classified information are required, under Executive Order 13587 and the National Policy on Insider Threat, to establish insider threat programs. The standards and guidelines that apply to insider threat programs in classified environments can also be employed effectively to improve the security of Controlled Unclassified Information in non-national security systems. Insider threat programs include controls to detect and prevent malicious insider activity through the centralized integration and analysis of both technical and non-technical information to identify potential insider threat concerns. A senior 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 as a minimum, 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 all offices within 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, for example, ongoing patterns of disgruntled behavior and conflicts with coworkers and other colleagues. These precursors can better inform and guide organizational officials in more focused, targeted monitoring efforts. However, the use of human resource records could raise significant concerns for privacy. The participation of a comprehensive legal team, including consultation with the senior agency officer for privacy (SAOP), ensures that all monitoring activities are performed in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines.

Related Controls: 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-1, PM-14.

Control Enhancements: None.

References: None.

PM-13 SECURITY AND PRIVACY WORKFORCE

Control: Establish a security and privacy workforce development and improvement program.

Supplemental Guidance: Security and privacy workforce development and improvement programs include, for example, defining the knowledge, skills, and abilities needed to perform security and

privacy duties and tasks; developing role-based training programs for individuals assigned security and privacy roles and responsibilities; and providing standards and guidelines for measuring and building individual qualifications for incumbents and applicants for security- and privacy-related positions. Such workforce development and improvement programs can also include security and privacy career paths to encourage security and privacy professionals to advance in the field and fill positions with greater responsibility. The programs encourage organizations to fill security- and privacy-related positions with qualified personnel. Security and privacy workforce development and improvement programs are complementary to organizational security awareness and training programs and focus on developing and institutionalizing the core security and privacy capabilities of personnel needed to protect organizational operations, assets, and individuals.

Related Controls: AT-2, AT-3.

Control Enhancements: None.

References: NIST Cyber Workforce Framework.

PM-14 TESTING, TRAINING, AND MONITORING

Control:

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 in a timely manner;

b. Review testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

Supplemental Guidance: This control ensures that organizations provide oversight for the security and privacy testing, training, and monitoring activities conducted organization-wide and that those activities are coordinated. With the growing importance of continuous monitoring programs, the implementation of information security and privacy across the three tiers of the risk management hierarchy and the widespread use of common controls, organizations coordinate and consolidate the testing and monitoring activities that are routinely conducted as part of ongoing organizational assessments supporting a variety of security and privacy controls. Security and privacy training activities, while focused on individual systems and specific roles, also necessitate coordination across all organizational elements. Testing, training, and monitoring plans and activities are informed by current threat and vulnerability assessments.

Related Controls: AT-2, AT-3, CA-7, CP-4, IR-3, PM-12, SI-4.

Control Enhancements: None.

References: NIST Special Publications 800-37, 800-39; 800-53A, 800-137.

PM-15 CONTACTS WITH ~~SECURITY~~ GROUPS AND ASSOCIATIONS

Control: 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-related information including threats, vulnerabilities, and incidents.

Supplemental Guidance: Ongoing contact with security and privacy groups and associations is of paramount importance in an environment of rapidly changing technologies and threats. Security and privacy groups and associations include, for example, special interest groups, professional

associations, forums, news groups, and peer groups of security and privacy professionals in similar organizations. Organizations select groups and associations based on organizational missions and business functions. Organizations share threat, vulnerability, privacy problems, contextual insights, compliance techniques, and incident information consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidelines.

Related Controls: SA-11, SI-5.

Control Enhancements: None.

References: None.

PM-16 THREAT AWARENESS PROGRAM

Control: Implement a threat awareness program that includes a cross-organization information-sharing capability.

Supplemental Guidance: Because of the constantly changing and increasing sophistication of adversaries, especially the advanced persistent threat (APT), it may be more likely that adversaries can successfully breach or compromise organizational systems. One of the best techniques to address this concern is for organizations to share threat information. This can include sharing threat events (i.e., tactics, techniques, and procedures) that organizations have experienced, mitigations that organizations have found are effective against certain types of threats, and threat intelligence (i.e., indications and warnings about threats that can occur). Threat information sharing may be bilateral or multilateral. Examples of bilateral threat sharing include government-commercial cooperatives and government-government cooperatives. An example of multilateral sharing includes organizations taking part in threat-sharing consortia. Threat information may be highly sensitive requiring special agreements and protection, or less sensitive and freely shared.

Related Controls: IR-4, PM-12.

Control Enhancements:

(1) THREAT AWARENESS PROGRAM | AUTOMATED MEANS FOR SHARING THREAT INTELLIGENCE

Utilize automated means to maximize the effectiveness of sharing threat intelligence information.

Supplemental Guidance: To maximize the effectiveness of monitoring, it is important to know what threat observables and indicators the sensors need to be searching for. By utilizing well established frameworks, services, and automated tools, organizations greatly improve their ability to rapidly share and feed into monitoring tools, the relevant threat detection signatures.

Related Controls: None.

References: None.

PM-17 PROTECTING CONTROLLED UNCLASSIFIED INFORMATION ON EXTERNAL SYSTEMS

Control:

a. Establish policy and procedures to ensure that the requirements for the protection of Controlled Unclassified Information processed, stored or transmitted on external systems, are implemented in accordance with applicable laws, Executive Orders, directives, policies, regulations, and standards.

b. Update the policy and procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: The protection of Controlled Unclassified Information (CUI) in nonfederal organizations and systems is critical to the security of federal operations and assets and the privacy of individuals. CUI is defined by the National Archives and Records Administration along with the appropriate safeguarding and dissemination requirements for such information and is codified in 32 CFR 2002, Controlled Unclassified Information and specifically, for systems external to the federal organization, in 32 CFR 2002.14h. The policy prescribes the specific use and conditions to be implemented in accordance with organizational procedures including, for example, via its contracting processes.

Related Controls: CA-6, PM-10.

Control Enhancements: None.

References: 32 CFR 2002; NIST Special Publication 800-171; NARA CUI Registry.

PM-18 PRIVACY PROGRAM PLAN

Control:

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 to address changes in federal privacy laws and policy and organizational changes and problems identified during plan implementation or privacy control assessments.

Supplemental Guidance: 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 and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks.

Privacy program plans can be integrated with information security plans or can be represented independently, either in a single document or in compilations of documents at the discretion of organizations. The plans document the program management controls and organization-defined common controls. Privacy program plans provide sufficient information about the program management and common controls (including specification of parameters and assignment and selection statements either 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.

The privacy plans for individual systems and the organization-wide privacy program plan together provide complete coverage for all 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.

Organizations have the flexibility to describe common controls in a single document or in multiple documents. In the case of multiple documents, the documents describing common controls are included as attachments to the privacy program plan. If the privacy program plan contains multiple documents, the organization specifies in each document, the organizational official or officials

responsible for the development, implementation, assessment, authorization, and monitoring of the respective common controls.

Related Controls: PM-8, PM-9, PM-19.

Control Enhancements: None.

References: None.

PM-19 PRIVACY PROGRAM ROLES

Control: Appoint a Senior Agency Official for Privacy with the authority, mission, accountability, and resources to coordinate, develop, and implement, applicable privacy requirements and manage privacy risks through the organization-wide privacy program.

Supplemental Guidance: The privacy officer described in this control is an organizational official. For federal agencies, as defined by applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines, this official is designated as the Senior Agency Official for Privacy. Organizations may also refer to this official as the Chief Privacy Officer.

Related Controls: PM-18, PM-21.

Control Enhancements: None.

References: None.

PM-20 SYSTEM OF RECORDS NOTICE

Control:

a. Publish System of Records Notices in the Federal Register, subject to required oversight processes, for systems containing personally identifiable information; and

b. Keep System of Records Notices current.

Supplemental Guidance: Organizations issue System of Records Notices to provide the public notice regarding personally identifiable information collected in a system of records. The Privacy Act defines a system of records as a group of any records under the control of any agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifier. System of Records Notices explain how the information is used, retained, and may be corrected, and whether certain portions of the system are subject to Privacy Act exemptions for law enforcement or national security reasons.

Related Controls: IP-5, PA-2, PA-3.

Control Enhancements: None.

References: None.

PM-21 DISSEMINATION OF PRIVACY PROGRAM INFORMATION

Control:

a. Ensure that the public has access to information about organizational privacy activities and can communicate with its Senior Agency Official for Privacy;

b. Ensure that organizational privacy practices are publicly available through organizational websites or otherwise; and

c. Employ 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.

Supplemental Guidance: Organizations employ different mechanisms for informing the public about

their privacy practices including, for example, Privacy Impact Assessments, System of Records Notices, privacy reports, publicly available web pages, email distributions, blogs, and periodic publications, including, for example, quarterly newsletters.

Related Controls: IP-4, IP-5, PM-19.

Control Enhancements: None.

References: None.

PM-22 ACCOUNTING OF DISCLOSURES

Control:

a. Develop and maintain an accounting of disclosures of personally identifiable information held in each system of records under its control, including:

   1. Date, nature, and purpose of each disclosure of a record; and

   2. Name and address of the person or organization to which the disclosure was made;

b. Retain the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer; and

c. Make the accounting of disclosures available to the person named in the record upon request.

Supplemental Guidance: This control addresses disclosure accounting requirements in the Privacy Act. The purpose of disclosure accounting requirements is to allow individuals to learn to whom records about them have been disclosed; to provide a basis for subsequently advising recipients of records of any corrected or disputed records; and to provide an audit trail for subsequent reviews of organizational compliance with conditions for disclosures. Organizations can use any system for keeping notations of disclosures, if it can construct from such a system, a document listing of all disclosures. Automated mechanisms can be used by organizations to determine when such information is disclosed, including, for example, commercial services providing notifications and alerts. Accounting of disclosures may also be used to help organizations verify compliance with applicable privacy statutes and policies governing disclosure or dissemination of information and dissemination restrictions.

Related Controls: AU-2.

Control Enhancements: None.

References: None.

PM-23 DATA QUALITY MANAGEMENT

Control: Issue guidelines ensuring and maximizing the quality, utility, objectivity, integrity, impact determination, and de-identification of personally identifiable information across the information life cycle.

Supplemental Guidance: Data quality management guidelines include the reasonable 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. Such steps may include, for example, editing and validating addresses as they are collected or entered into systems using automated address verification look-up application programming interfaces. The measures taken to protect data quality are based on the nature and context of the personally identifiable information, how it is to be used, how it was obtained, the impact level of the personally identifiable information obtained, and potential de-identification methods employed. Measures taken to validate the accuracy of personally identifiable information that is used to make determinations about the rights, benefits, or privileges of individuals under federal programs may be more comprehensive than those used to validate less sensitive personally identifiable information. Additional steps may be necessary to validate personally identifiable

information that is obtained from sources other than individuals or the authorized representatives of individuals.

Related Controls: PM-24, SI-20.

Control Enhancements:

(1) DATA QUALITY MANAGEMENT | AUTOMATION

Issue technical guidelines and documentation to support automated evaluation of data quality across the information life cycle.

Supplemental Guidance: 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 tools and techniques can augment existing process 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 auditing of data, to track how data is used across the information life cycle, and to detect errors that may incorrectly alter personally identifiable information or incorrectly associate such information with the wrong individual. These automated capabilities backstop processes and procedures at-scale. They also enable more fine-grained detection and correction of data quality errors.

Related Controls: None.

(2) DATA QUALITY MANAGEMENT | DATA TAGGING

Issue data modeling guidelines to support tagging of personally identifiable information.

Supplemental Guidance: Data tagging includes, for example, tags noting the authority to collect, usage, presence of personally identifiable information, de-identification, impact level, and information life cycle stage.

Related Controls: SC-16.

(3) DATA QUALITY MANAGEMENT | UPDATING PERSONALLY IDENTIFIABLE INFORMATION

When managing personally identifiable information, develop procedures and incorporate mechanisms to identify and record the method under which the information is updated, and the frequency that such updates occur.

Supplemental Guidance: When managing personally identifiable information including, for example, health information and financial information, it is important to carefully track updates or changes to such data. Having the ability to track both the method and frequency of updates enhances transparency and individual participation. It also enables individuals to better understand how and when their information is changed and helps both individuals and the responsible organizations to know how and what personally identifiable information was changed should erroneous information be identified.

Related Controls: None.

References: NIST Special Publication 800-188.

PM-24 DATA MANAGEMENT BOARD

Control:

a. Establish a written charter for a Data Management Board;

b. Establish the Data Management Board consisting of [*Assignment: organization-defined roles*] with the following responsibilities:

1. Develop and implement guidelines supporting data modeling, quality, integrity, and de-identification needs of personally identifiable information across the information life cycle;

2. Review and approve applications to release data outside of the organization, archiving the applications and the released data, and performing post-release monitoring to ensure that the assumptions made as part of the data release continue to be valid;

c. Include requirements for personnel interaction with the Data Management Board in security and privacy awareness and/or role-based training.

Supplemental Guidance: The guidelines established by Data Management Board establish policies, procedures, and standards that enable data governance so that personally identifiable information is managed and maintained in accordance with any relevant statutes, regulations, and guidance. Members may include the Chief Information Officer, Senior Agency Information Security Officer, and Senior Agency Official for Privacy. With respect to data modeling, and the quality, integrity, and de-identification of personally identifiable information, data and information needs are met through organization-wide data governance policies that establish the roles, responsibilities, and processes by which personnel manage information as an asset across the information life cycle. The information life cycle includes creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposition. Members may include the Chief Information Officer, Senior Agency Official for Privacy, and Senior Agency Information Security Officer.

Related Controls: AT-2, AT-3, PM-23, PM-25, SI-4, SI-20.

Control Enhancements: None.

References: NIST Special Publication 800-188.

PM-25 DATA INTEGRITY BOARD

Control: Establish a Data Integrity Board to oversee organizational Computer Matching Agreements.

Supplemental Guidance: Organizations executing Computer Matching Agreements or participating in such agreements with other organizations regarding applicants for and recipients of financial assistance or payments under federal benefit programs or certain computerized comparisons involving federal personnel or payroll records, establish a Data Integrity Board to oversee and coordinate the implementation of those matching agreements. As data is obtained and used across the information life cycle, it is important to confirm the accuracy and relevance of personally identifiable information. Organizations may integrate the function of the Data Integrity Board into the responsibilities of the Data Management Board under PM-24. In many organizations, the Data Integrity Board is led by the Senior Agency Official for Privacy.

Related Controls: AC-1, AC-3, AC-4, AU-2, AU-3, AU-6, AU-11, PA-2, PA-4, PM-24, SC-8, SC-28, SI-19, SI-20.

Control Enhancements:

(1) DATA INTEGRITY BOARD | PUBLISH AGREEMENTS ON WEBSITE

Publish Computer Matching Agreements on the public website of the organization.

Supplemental Guidance: None.

Related Controls: None.

References: None.

PM-26 MINIMIZATION OF PERSONALLY IDENTIFIABLE INFORMATION USED IN TESTING, TRAINING, AND RESEARCH

Control:

a. Develop and implement policies and procedures that address the use of personally identifiable information for internal testing, training, and research;

b. Take measures to limit or minimize the amount of personally identifiable information used for internal testing, training, and research purposes; and

c. Authorize the use of personally identifiable information when such information is required for internal testing, training, and research.

Supplemental Guidance: Organizations often use personally identifiable information for testing new applications or systems prior to deployment, for research purposes, and for training. The use of personally identifiable information in testing, research, and training increases risk of unauthorized disclosure or misuse of such information. Organizations consult with the Senior Agency Official for Privacy and legal counsel to ensure that the use of personally identifiable information in testing, training, and research is compatible with the original purpose for which it was collected. When possible, organizations use placeholder data to avoid exposure of personally identifiable information when conducting testing, training, and research.

Related Controls: PA-3.

Control Enhancements: None.

References: None.

PM-27 INDIVIDUAL ACCESS CONTROL

Control:

a. Publish:

1. Policies governing how individuals may request access to records maintained in a Privacy Act system of records; and

2. Access procedures in System of Records Notices; and

b. Ensure that the published policies and access procedures are consistent with Privacy Act requirements and Office of Management and Budget policies and guidance for the proper processing of Privacy Act requests.

Supplemental Guidance: Access affords individuals the ability to review personally identifiable information about them held within organizational systems of records. Access includes timely, simplified, and inexpensive access to data. Organizational processes for allowing access to records may differ based on resources, legal requirements, or other factors. The Senior Agency Official for Privacy is responsible for the content of Privacy Act regulations and record request processing, in consultation with the organization's legal counsel. Access to certain types of records may not be appropriate, however, and heads of agencies may promulgate rules exempting particular systems from the access provision of the Privacy Act.

Related Controls: IP-6.

Control Enhancements: None.

References: None.

PM-28 COMPLAINT MANAGEMENT

Control: Implement a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational 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; and

c. Tracking mechanisms to ensure all complaints received are reviewed and appropriately addressed in a timely manner.

Supplemental Guidance: Complaints, concerns, and questions from individuals can serve as a valuable source of external input that ultimately improves operational models, uses of technology, data collection practices, and privacy and security controls. Mechanisms that can be used by the public may include, for example, e-mail, telephone hotline, or web-based forms. Information necessary for successfully filing complaints includes, for example, contact information for the Senior Agency Official for Privacy or other official designated to receive complaints.

Related Controls: IP-3, IR-7, IR-9.

Control Enhancements: None.

References: None.

PM-29 INVENTORY OF PERSONALLY IDENTIFIABLE INFORMATION

Control:

a. Establish, maintain, and update [*Assignment: organization-defined frequency*] an inventory of all programs and systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of personally identifiable information;

b. Provide updates of the personally identifiable information inventory to the Chief Information Officer, Senior Agency Official for Privacy, and Senior Agency Information Security Officer [*Assignment: organization-defined frequency*];

c. Use the personally identifiable information inventory to support the establishment of information security and privacy requirements for all new or modified systems containing personally identifiable information;

d. Review the personally identifiable information inventory [*Assignment: organization-defined frequency*];

e. Ensure to the extent practicable, that personally identifiable information is accurate, relevant, timely, and complete; and

f. Reduce personally identifiable information to the minimum necessary for the proper performance of authorized organizational functions.

Supplemental Guidance: Organizations coordinate with federal records officers to ensure that reductions in organizational holdings of personally identifiable information are consistent with National Archives and Records Administration retention schedules. By performing periodic assessments, organizations ensure that only the data specified in the notice is collected, and that the data collected is still relevant and necessary for the purpose specified in privacy notices. The set of personally identifiable information elements required to support an organizational mission or business process may be a subset of the personally identifiable information the organization is authorized to collect.

Related Controls: CM-8, PL-8.

Control Enhancements:

(1) INVENTORY OF PERSONALLY IDENTIFIABLE INFORMATION | AUTOMATION SUPPORT

Employ automated mechanisms to determine if personally identifiable information is maintained in electronic form.

Supplemental Guidance: Automated mechanisms include, for example, commercial services providing notifications and alerts to organizations about where personally identifiable information is stored.

Related Controls: None.

References: None.

PM-30 PRIVACY REPORTING

Control: Develop, disseminate, and update privacy reports to:

a. The Office of Management and Budget, Congress, and other oversight bodies to demonstrate accountability with statutory and regulatory privacy program mandates; and

b. [*Assignment: organization-defined officials*] and other personnel with responsibility for monitoring privacy program progress and compliance.

Supplemental Guidance: Through internal and external privacy reporting, organizations promote accountability and transparency in organizational privacy operations. Reporting can also help organizations to determine progress in meeting privacy compliance requirements and privacy controls, compare performance across the federal government, identify vulnerabilities and gaps in policy and implementation, and identify success models. Privacy reports include, for example, annual Senior Agency Official for Privacy reports to OMB; reports to Congress required by the Implementing Regulations of the 9/11 Commission Act; and other public reports required by specific statutory mandates or internal policies of organizations. The Senior Agency Official for Privacy consults with legal counsel, where appropriate, to ensure that organizations meet all applicable privacy reporting requirements.

Related Controls: IR-9, PM-19.

Control Enhancements: None.

References: None.

PM-31 SUPPLY CHAIN RISK MANAGEMENT PLAN

Control:

a. Develop a plan for managing supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services;

b. Implement the supply chain risk management plan consistently across the organization; and

c. Review and update the supply chain risk management plan [*Assignment: organization-defined frequency*] or as required, to address organizational changes.

Supplemental Guidance: An organization-wide supply chain risk management plan includes, for example, an unambiguous 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 supply chain risk management plan, and associated roles and responsibilities. The organization-wide supply chain risk management plan can be incorporated into the organization's risk management strategy and be used to inform the system-level supply chain risk management plan. The use of a risk executive function can facilitate consistent, organization-wide application of the supply chain risk management plan.

Related Controls: PM-9, SA-12.

Control Enhancements: None.

References: NIST Special Publication 800-161.

PM-32 RISK FRAMING

Control:

a. Identify assumptions affecting risk assessments, risk response, and risk monitoring;

b. Identify constraints affecting risk assessments, risk response, and risk monitoring;

c. Identify the organizational risk tolerance; and

d. Identify priorities and trade-offs considered by the organization for managing risk.

Supplemental Guidance: Risk framing is most effectively conducted at the organization-wide level. The assumptions, constraints, organizational risk tolerance, and priorities and trade-offs identified for this control inform the organizational risk management strategy which in turn, informs the conduct of risk assessment, risk response, and risk monitoring.

Related Controls: CA-7, PM-9, RA-3, RA-7.

Control Enhancements: None.

References: NIST Special Publication 800-39.

3.16 PERSONNEL SECURITY

Quick link to Personnel Security summary table

PS-1 PERSONNEL SECURITY POLICY AND PROCEDURES

Control:

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

1. A 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 senior management official*] to manage the personnel security policy and procedures;

~~b.~~c. Review and update the current personnel security:

1. Policy [*Assignment: organization-defined frequency*]; and

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

d. Ensure that the personnel security procedures implement the personnel security policy and controls; and

e. Develop, document, and implement remediation actions for violations of the personnel security policy.

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of ~~selected security~~the controls and control enhancements in the PS family. The risk management strategy is an important factor in establishing policy and procedures ~~reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards,~~. Comprehensive policy and ~~guidance.~~procedures help provide security and privacy assurance. Security and privacy program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general ~~information~~ security and privacy policy ~~for organizations~~ or ~~conversely,~~ can be represented by multiple policies reflecting the complex nature of ~~certain~~ organizations. The procedures can be established for security ~~program in general~~and privacy programs and for ~~particular information~~ systems, if needed. ~~The~~Procedures describe how policies or controls are implemented and can be directed at the personnel 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. It is important to recognize that restating controls does not constitute an organizational ~~risk management strategy is a key factor in establishing~~ policy ~~and procedures~~or procedure.

Related Controls: PM-9, PS-8, SI-12.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-30, 800-39, 800-100.

PS-2 POSITION RISK DESIGNATION

Control:

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*].

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

Related Controls: AC-5, AT-3, PE-2, PE-3, PL-2, PS-3, PS-6, SA-5, SA-21, SI-12.

Control Enhancements: None.

References: 5 C.F.R. 731.106.

PS-3 PERSONNEL SCREENING

Control:

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*].

Supplemental Guidance: Personnel screening and rescreening activities reflect applicable laws, Executive Orders, directives, regulations, policies, standards, guidelines, and specific criteria established for the risk designations of assigned positions. Organizations may define different rescreening conditions and frequencies for personnel accessing systems based on types of information processed, stored, or transmitted by the systems.

Related Controls: AC-2, IA-4, MA-5, PE-2, PM-12, PS-2, PS-6, PS-7, SA-21.

Control Enhancements:

(1) PERSONNEL SCREENING | CLASSIFIED INFORMATION

Verify that individuals accessing a system processing, storing, or transmitting classified information are cleared and indoctrinated to the highest classification level of the information to which they have access on the system.

Supplemental Guidance: None.

Related Controls: AC-3, AC-4.

(2) PERSONNEL SCREENING | FORMAL INDOCTRINATION

Verify that individuals accessing a system processing, storing, or transmitting types of classified information which require formal indoctrination, are formally indoctrinated for all the relevant types of information to which they have access on the system.

Supplemental Guidance: Types of classified information requiring formal indoctrination include, for example, Special Access Program (SAP), Restricted Data (RD), and Sensitive Compartment Information (SCI).

Related Controls: AC-3, AC-4.

(3) PERSONNEL SCREENING | INFORMATION WITH SPECIAL PROTECTION 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*].

Supplemental Guidance: Organizational information requiring special protection includes, for example, Controlled Unclassified Information (CUI~~) and Sources and Methods Information (SAMI).~~). Personnel security criteria include, for example, position sensitivity background screening requirements.

Related Controls: None.

(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*].

Supplemental Guidance: None.

Related Controls: None.

References: FIPS Publications 199, 201; NIST Special Publications 800-60-1, 800-60-2, 800-73, 800-76, 800-78.

PS-4 PERSONNEL TERMINATION

Control: 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;

e. Retain access to organizational information and systems formerly controlled by terminated individual; and

f. Notify [*Assignment: organization-defined personnel or roles*] within [*Assignment: organization-defined time-period*].

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

Related Controls: AC-2, IA-4, PE-2, PM-12, PS-6, PS-7.

Control Enhancements:

(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.

Supplemental Guidance: Organizations consult with the Office of the General Counsel regarding matters of post-employment requirements on terminated individuals.

Related Controls: None.

(2) PERSONNEL TERMINATION | AUTOMATED NOTIFICATION

Employ automated mechanisms to notify [*Assignment: organization-defined personnel or roles*] upon termination of an individual.

Supplemental Guidance: 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 specific organizational personnel or roles ~~(e.g., management personnel, supervisors, personnel security officers, information security officers,~~

~~systems administrators, or information technology administrators)~~ when individuals are terminated. Such automatic alerts or notifications can be conveyed in a variety of ways, including, for example, telephonically, via electronic mail, via text message, or via websites.

Related Controls: None.

References: None.

PS-5 PERSONNEL TRANSFER

Control:

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*].

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

Related Controls: AC-2, IA-4, PE-2, PM-12, PS-4, PS-7.

Control Enhancements: None.

References: None.

PS-6 ACCESS AGREEMENTS

Control:

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*].

Supplemental Guidance: Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Signed access agreements include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with organizational systems to which access is authorized. Organizations can use electronic signatures to acknowledge access agreements unless specifically prohibited by organizational policy.

Related Controls: AC-17, PE-2, PL-4, PS-2, PS-3, PS-7, PS-8, SA-21, SI-12.

Control Enhancements:

(1) ACCESS AGREEMENTS | INFORMATION REQUIRING SPECIAL PROTECTION

[Withdrawn: Incorporated into PS-3].

(2) ACCESS AGREEMENTS | CLASSIFIED INFORMATION REQUIRING SPECIAL PROTECTION

~~ensures~~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.

Supplemental Guidance: Classified information requiring special protection includes, for example, 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.

Related Controls: None.

(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.

Supplemental Guidance: Organizations consult with the Office of the General Counsel regarding matters of post-employment requirements on terminated individuals.

Related Controls: PS-4.

References: None.

PS-7 EXTERNAL PERSONNEL SECURITY

Control:

a. Establish personnel security requirements including security roles and responsibilities for ~~third-party~~external providers;

b. ~~third-party~~Require external providers to comply with personnel security policies and procedures established by the organization;

c. Document personnel security requirements;

d. ~~third-party~~Require external providers to notify [*Assignment: organization-defined personnel or roles*] of any personnel transfers or terminations of ~~third-party~~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.

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

Related Controls: AT-2, AT-3, MA-5, PE-3, PS-2, PS-3, PS-4, PS-5, PS-6, SA-5, SA-9, SA-21.

Control Enhancements: None.

References: NIST Special Publication 800-35.

PS-8 PERSONNEL SANCTIONS

Control:

a. Employ a formal sanctions process for individuals failing to comply with established information security 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.

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

Related Controls: All XX-1 Controls, IP-1, PL-4, PM-12, PS-6.

Control Enhancements: None.

References: None.

3.17 RISK ASSESSMENT

Quick link to Risk Assessment summary table

RA-1 RISK ASSESSMENT POLICY AND PROCEDURES

Control:

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

1. A 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 senior management official*] to manage the risk assessment policy and procedures;

~~b.~~c. Review and update the current risk assessment:

1. Policy [*Assignment: organization-defined frequency*]; and

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

d. Ensure that the risk assessment procedures implement the risk assessment policy and controls; and

e. Develop, document, and implement remediation actions for violations of the risk assessment policy.

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of ~~selected security~~ the controls and control enhancements in the RA family. The risk management strategy is an important factor in establishing policy and procedures ~~reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards,~~. Comprehensive policy and ~~guidance.~~procedures help provide security and privacy assurance. Security and privacy program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general ~~information~~ security and privacy policy ~~for organizations~~ or ~~conversely,~~ can be represented by multiple policies reflecting the complex nature of ~~certain~~ organizations. The procedures can be established for ~~the~~ security ~~program in general~~and privacy programs and for ~~particular information~~ systems, if needed. ~~The~~Procedures describe how policies or controls are implemented and can be directed at the personnel 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. It is important to recognize that restating controls does not constitute an organizational ~~risk management strategy is a key factor in establishing~~ policy ~~and procedures.~~ or procedure.

Related Controls: PM-9, PS-8, SI-12.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-30, 800-39, 800-100.

RA-2 SECURITY CATEGORIZATION

Control:

~~a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;~~

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. ~~Ensures~~Verify that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.

Supplemental Guidance: Clearly defined authorization boundaries are a prerequisite for effective security categorization decisions. Security categories describe the potential adverse impacts to organizational operations, organizational assets, and individuals if organizational information and systems are comprised through a loss of confidentiality, integrity, or availability. Organizations conduct the security categorization process as an organization-wide activity with the involvement of Chief Information Officers, Senior ~~information security officers, information~~Agency Information Security Officers, system owners, mission and business owners, and information owners/stewards. Organizations also consider the potential adverse impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level adverse impacts. Security categorization processes ~~carried out by organizations~~ facilitate the development of inventories of information assets, and along with CM-8, mappings to specific system components where information is processed, stored, or transmitted.

Related Controls: CM-8, MP-4, PL-2, PL-10, PL-11, PM-7, RA-3, RA-5, RA-7, SC-7, SC-38, SI-12.

Control Enhancements:

(1) SECURITY CATEGORIZATION | SECOND-LEVEL CATEGORIZATION

Conduct a second-level categorization of organizational systems to obtain additional granularity on system impact levels.

Supplemental Guidance: Organizations apply the "high water mark" concept to each of their systems categorized in accordance with FIPS Publication 199. This process results in systems designated as low impact, moderate impact, or high impact. Organizations desiring additional granularity in the system impact designations for risk-based decision making, can further partition the systems into sub-categories of the initial, first-level system categorization. For example, a second-level categorization on a moderate-impact system can produce three new sub-categories: low-moderate systems, moderate-moderate systems, and high-moderate systems. This secondary categorization and the resulting sub-categories of the system give organizations an opportunity to further prioritize their investments related to security control selection and the tailoring of control baselines in responding to identified risks. Second-level categorization can also be used to determine those systems that are exceptionally critical to organizational missions and business operations. These systems are sometimes described as high-value assets and thus, organizations may be more focused on complexity, aggregation, and interconnections. Such systems can be identified by partitioning high-impact systems into low-high systems, moderate-high systems, and high-high systems.

Related Controls: None.

References: FIPS Publications 199, 200; NIST Special Publications 800-30, 800-39, 800-60-1, 800-60-2.

RA-3 RISK ASSESSMENT

Control:

a. Conduct a risk assessment, including the likelihood and magnitude of harm, from:

1. The unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and

2. Privacy-related problems for individuals arising from the intentional processing of personally identifiable information;

b. Integrate risk assessment results and risk management decsions from the organization and missions/business process perspectives with system-level risk assessments;

~~b.~~c. Document risk assessment results in [*Selection: security and privacy plans; risk assessment report;* [*Assignment: organization-defined document*]];

~~c.~~d. Review risk assessment results [*Assignment: organization-defined frequency*];

~~d.~~e. Disseminate risk assessment results to [*Assignment: organization-defined personnel or roles*]; and

~~e.~~f. Update the risk assessment [*Assignment: organization-defined frequency*] or when there are significant changes to the system, its environment of operation ~~(including the identification of new threats and vulnerabilities),~~ or other conditions that may impact the security or privacy state of the system.

Supplemental Guidance: Clearly defined authorization boundaries are a prerequisite for effective risk assessments. Risk assessments consider threats, vulnerabilities, likelihood, and impact to organizational operations and assets, individuals, other organizations, and the Nation based on the operation and use of systems. Risk assessments also take into account risk from external parties ~~(e.g., service providers,~~including, for example, individuals accessing organizational systems; contractors operating ~~information~~ systems on behalf of the organization~~, individuals accessing organizational information systems,~~; service providers; and outsourcing entities~~). In accordance with OMB policy and related E-authentication initiatives, authentication of public users accessing federal information systems may also be required to protect nonpublic or privacy-related information. As such, organizational assessments of risk also address public access to federal information systems~~.

Organizations can conduct risk assessments, either formal or informal, at all three tiers in the risk management hierarchy (i.e., organization level, mission/business process level, or system level) and at any phase in the system development life cycle. Risk assessments can also be conducted at various steps in the Risk Management Framework, including categorization, control selection, control implementation, control assessment, system authorization, and ~~security control monitoring. RA-3 is noteworthy in that the control must be partially implemented prior to the implementation of other controls in order to complete the first two steps in the Risk Management Framework. Risk assessments~~control monitoring. In addition to the information processed, stored, and transmitted by the system, risk assessments can also address any information related to the system including, for example, system design, the intended use of the system, testing results, and other supply chain-related information or artifacts. Assessments of risk can play an important role in security and privacy control selection processes, particularly during the application of tailoring guidance~~, which includes security control supplementation.~~ .

Related Controls: CA-3, CP-6, CP-7, IA-8, MA-5, PE-3, PE-18, PL-2, PL-10, PL-11, PM-8, PM-9, PM-32, RA-2, RA-5, RA-7, SA-9, SC-38, SI-12.

Control Enhancements:

(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.

Supplemental Guidance: Supply chain-related events include, for example, disruption, theft, use of defective components, insertion of counterfeits, malicious development practices, improper delivery practices, and insertion of malicious code. These events can have a significant impact on the confidentiality, integrity, or availability of a system and its information and therefore, can also adversely impact organizational operations (including mission, functions, image, or

reputation), organizational assets, individuals, other organizations, and the Nation. The supply chain-related events may be unintentional or malicious and can occur at any point during the system life cycle. An analysis of supply chain risk can help an organization identify systems or components for which additional supply chain risk mitigations are required.

Related Controls: RA-2, RA-9, PM-17, SA-12.

References: NIST Special Publications 800-30, 800-39, 800-161; NIST Interagency Report 8023.

RA-4 RISK ASSESSMENT UPDATE

[Withdrawn: Incorporated into RA-3].

RA-5 VULNERABILITY SCANNING

Control:

a. 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~~/applications~~ are identified and reported;

b. Employ vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:

   1. Enumerating platforms, software flaws, and improper configurations;

   2. Formatting checklists and test procedures; and

   3. Measuring vulnerability impact;

c. Analyze vulnerability scan reports and results from control assessments;

d. Remediate legitimate vulnerabilities [*Assignment: organization-defined response times*] in accordance with an organizational assessment of risk;

e. Share information obtained from the vulnerability scanning process and control assessments with [*Assignment: organization-defined personnel or roles*] to help eliminate similar vulnerabilities in other ~~(i.e., systemic weaknesses or deficiencies).~~systems; and

f. Employ vulnerability scanning tools that include the capability to readily update the vulnerabilities to be scanned.

Supplemental Guidance: Security categorization of information and systems guides the frequency and comprehensiveness of vulnerability scans. Organizations determine the required vulnerability scanning for system components, ensuring that the potential sources of vulnerabilities such as networked printers, scanners, and copiers are not overlooked. The vulnerabilities to be scanned need to be readily updated as new vulnerabilities are discovered, announced, and scanning methods developed. ~~Vulnerability analyses for custom software applications~~This process helps to ensure that potential vulnerabilities in the system are identified and addressed as quickly as possible. Vulnerability 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, for example, web-based application scanners, static analysis tools, and binary analyzers. Vulnerability scanning includes, for example, scanning for patch levels; scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and scanning for improperly configured or incorrectly operating information flow control mechanisms. Scanning tools that facilitate interoperability include, for example, products 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 use the Open Vulnerability Assessment Language (OVAL) to determine~~/test for~~ the presence of vulnerabilities. ~~Suggested~~ Sources for vulnerability information include, for example, the Common Weakness Enumeration (CWE) listing and the National Vulnerability Database

(NVD). Control assessments such as red team exercises provide additional sources of potential vulnerabilities for which to scan. Organizations also consider using scanning tools that express vulnerability impact by the Common Vulnerability Scoring System (CVSS).

Related Controls: CA-2, CA-7, CM-2, CM-4, CM-6, CM-8, RA-2, RA-3, SA-11, SA-12, SA-15, SC-38, SI-2, SI-3, SI-4, SI-7.

Control Enhancements:

(1) VULNERABILITY SCANNING | UPDATE TOOL CAPABILITY

~~**The organization employs vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned.**~~

~~Supplemental Guidance: [Withdrawn: Incorporated into RA-5].~~

~~**(2)** The vulnerabilities to be scanned need to be readily updated as new vulnerabilities are discovered, announced, and scanning methods developed. This updating process helps to ensure that potential vulnerabilities in the information system are identified and addressed as quickly as possible. Related controls: SI-3, SI-7.~~

(3)(2) VULNERABILITY SCANNING | UPDATE BY FREQUENCY~~/~~, PRIOR TO NEW SCAN, OR WHEN IDENTIFIED

Update the system vulnerabilities to be scanned [*Selection (one or more):* [*Assignment: organization-defined frequency*]; *prior to a new scan; when new vulnerabilities are identified and reported*].

Supplemental Guidance: None.

Related Controls: SI-5.

(4)(3) VULNERABILITY SCANNING | BREADTH AND DEPTH OF COVERAGE

Employ vulnerability scanning procedures that can identify the breadth and depth of coverage.

Supplemental Guidance: The identification of the breadth and depth of coverage can include, for example, the system components scanned and the vulnerabilities checked.

Related Controls: None.

(5)(4) VULNERABILITY SCANNING | DISCOVERABLE INFORMATION

Determine unintended discoverable information about the ~~information~~ system ~~is discoverable by adversaries~~ and ~~subsequently takes~~take [*Assignment: organization-defined corrective actions*].

Supplemental Guidance: Discoverable information includes information that adversaries could obtain without directly compromising or breaching the system, for example, by collecting information the system is exposing or by conducting extensive searches of the web. Corrective actions can include, for example, notifying appropriate organizational personnel, removing designated information, or changing the system to make designated information less relevant or attractive to adversaries.

Related Controls: AU-13.

(6)(5) VULNERABILITY SCANNING | PRIVILEGED ACCESS

Implements privileged access authorization to [*Assignment: organization-identified system components*] for [*Assignment: organization-defined vulnerability scanning activities*].

Supplemental Guidance: 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 ~~highly sensitive~~classified or controlled unclassified information. Privileged access authorization to selected system components facilitates more thorough vulnerability scanning and protects the sensitive nature of such scanning.

Related Controls: None.

(7)(6) VULNERABILITY SCANNING | AUTOMATED TREND ANALYSES

Employ automated mechanisms to compare the results of vulnerability scans over time to determine trends in system vulnerabilities.

Supplemental Guidance: None.

Related Controls: None.

~~(8)~~(7) VULNERABILITY SCANNING | AUTOMATED DETECTION AND NOTIFICATION OF UNAUTHORIZED COMPONENTS

[Withdrawn: Incorporated into CM-8].

~~(9)~~(8) VULNERABILITY SCANNING | REVIEW HISTORIC AUDIT LOGS

Review historic audit logs to determine if a vulnerability identified in the system has been previously exploited.

Supplemental Guidance: None.

Related Controls: AU-6, AU-11.

~~(10)~~(9) VULNERABILITY SCANNING | PENETRATION TESTING AND ANALYSES

[Withdrawn: Incorporated into CA-8].

~~(11)~~(10) VULNERABILITY SCANNING | CORRELATE SCANNING INFORMATION

Correlate the output from vulnerability scanning tools to determine the presence of multi-vulnerability and multi-hop attack vectors.

Supplemental Guidance: None.

Related Controls: None.

References: NIST Special Publications 800-40, 800-70, 800-115, 800-126; NIST Interagency Reports 7788, 8023.

RA-6 TECHNICAL SURVEILLANCE COUNTERMEASURES SURVEY

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

Supplemental Guidance: Technical surveillance countermeasures surveys are performed by qualified personnel. Organizations use such surveys to detect the presence of technical surveillance devices~~/~~ and hazards and to identify technical security weaknesses that could aid in the conduct of technical penetrations of surveyed facilities. ~~Such~~In addition, technical surveillance countermeasures surveys provide evaluations of the technical security ~~postures~~posture of organizations and facilities and ~~typically~~ include thorough visual, electronic, and physical examinations ~~in and about~~of surveyed facilities~~.~~, both internally and externally. The surveys also provide useful input ~~into~~for organizational risk assessments and critical information regarding organizational exposure to potential adversaries.

Related Controls: None.

Control Enhancements: None.

References: None.

RA-7 RISK RESPONSE

Control: Respond to findings from security and privacy assessments, monitoring, and audits.

Supplemental Guidance: Organizations have a variety of options for responding to risk including: mitigating the risk by implementing new controls or strengthening existing controls; accepting the risk with appropriate justification or rationale; sharing or transferring the risk; or rejecting the risk. Organizational risk tolerance influences risk response decisions and actions. Risk response is also known as risk treatment. This control addresses the need to determine an appropriate response to risk before a plan of action and milestones entry is generated. For example, the response may be to accept risk or reject risk, or it may be possible to mitigate the risk immediately so a plan of action and milestones entry is not needed. However, if the risk response is to mitigate the risk and the mitigation cannot be completed immediately, a plan of action and milestones entry is generated.

Related Controls: CA-5, IR-9, PM-4, PM-32, RA-2, RA-3.

Control Enhancements: None.

References: FIPS Publications 199, 200; NIST Special Publications 800-30, 800-37, 800-39, 800-160.

RA-8 PRIVACY IMPACT ASSESSMENTS

Control: Conduct privacy impact assessments for systems, programs, or other activities that pose a privacy risk before:

a. Developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form; and

b. Initiating a new collection of information that:

   1. Will be collected, maintained, or disseminated using information technology; and

   2. Includes information in an identifiable form permitting the physical or online contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, ten or more persons, other than agencies, instrumentalities, or employees of the Federal Government.

Supplemental Guidance: Privacy impact assessments are an analysis of how information is managed to ensure that such management conforms to applicable legal, regulatory, and policy requirements regarding privacy; to determine the associated privacy risks and effects of creating, collecting, using, processing, storing, maintaining, disseminating, disclosing, and disposing of information in identifiable form in a system; and to examine and evaluate the protections and alternate processes for managing information to mitigate potential privacy concerns. A privacy impact assessment is an analysis and a formal document detailing the process and outcome of the analysis. To conduct the analysis, organizations use risk assessment processes. Although privacy impact assessments may be required by law, organizations may develop policies to require privacy impact assessments in circumstances where a privacy impact assessment would not be required by law.

Related Controls: IP-4, PA-2, PA-3, RA-1, RA-3, RA-7.

Control Enhancements: None.

References: None.

RA-9 CRITICALITY ANALYSIS

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

Supplemental Guidance: Not all system components, functions, or services necessarily require significant protections. Criticality analysis is a key tenet of, for example, supply chain risk management, and informs the prioritization of protection activities. The identification of critical system components and functions considers applicable regulations, directives, policies, standards, and guidelines, system functionality requirements, system and component interfaces, and system and component dependencies. Systems engineers conduct an end-to-end functional decomposition of a system to identify mission-critical functions and components. The functional decomposition includes the identification of core 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 beyond the system boundary.

The operational environment of a system or component may impact the criticality including, for example, 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 such components create. Component and function criticality are assessed in terms of the impact of a component or function failure on the organizational missions supported by the system containing

those components and functions. A criticality analysis is performed when an architecture or design is being developed, modified, or upgraded. If done early in the system life cycle, organizations may consider modifying the system design to reduce the critical nature of these components and functions by, for example, adding redundancy or alternate paths into the system design.

Related Controls: CP-2, PL-2, PL-8, PL-11, PM-1, SA-8, SA-12, SA-15, SA-20.

Control Enhancements: None.

References: None.

3.18 SYSTEM AND SERVICES ACQUISITION

Quick link to System and Services Acquisition summary table

SA-1 SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES

Control:

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

1. A 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 senior management official*] to manage the system and services acquisition policy and procedures;

c. Review and update the current system and services acquisition:

1. Policy [*Assignment: organization-defined frequency*]; and

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

d. Ensure that the system and services acquisition procedures implement the system and services acquisition policy and controls; and

e. Develop, document, and implement remediation actions for violations of the system and services acquisition policy.

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of ~~selected security~~ the controls and control enhancements in the SA family. The risk management strategy is an important factor in establishing policy and procedures ~~reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards,~~. Comprehensive policy and ~~guidance.~~procedures help provide security and privacy assurance. Security and privacy program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general ~~information~~ security and privacy policy ~~for organizations~~ or ~~conversely,~~ can be represented by multiple policies reflecting the complex nature of ~~certain~~ organizations. The procedures can be established for ~~the~~ security ~~program in general~~and privacy programs and for ~~particular information~~ systems, if needed. ~~The~~Procedures describe how policies or controls are implemented and can be directed at the personnel 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. It is important to recognize that restating controls does not constitute an organizational ~~risk management strategy is a key factor in establishing policy and procedures.~~ policy or procedure.

Related Controls: PM-9, PS-8, SI-12.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-30, 800-39, 800-100.

SA-2 ALLOCATION OF RESOURCES

Control:

a. Determine 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.

Supplemental Guidance: Resource allocation for information security and privacy includes funding for ~~the initial~~ system or ~~system~~ service acquisition ~~and funding for the~~, sustainment ~~of~~, and supply chain concerns throughout the system~~/service.~~ development life cycle.

Related Controls: PL-7, PM-3, PM-11, SA-9.

Control Enhancements: None.

References: NIST Special Publication 800-65.

SA-3 SYSTEM DEVELOPMENT LIFE CYCLE

Control:

a. 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.

Supplemental Guidance: A ~~well-defined~~ system development life cycle process provides the foundation for the successful development, implementation, and operation of organizational ~~information~~ systems. To apply the required security and privacy controls within the system development life cycle requires a basic understanding of information security and privacy, threats, vulnerabilities, adverse impacts, and risk to critical missions and business functions. The security engineering principles in SA-8 ~~cannot be properly applied if~~ help individuals ~~that~~properly design, code, and test systems and system components ~~(including information technology products) do not understand security~~. Organizations include qualified personnel including, for example, chief information security officers, security architects, security engineers, system security officers, and chief privacy officers in system development life cycle processes to ensure that established security and privacy requirements are incorporated into organizational systems. It is also important that developers include individuals on the development team that possess the requisite security and privacy expertise and skills to ensure that the needed security and privacy capabilities are effectively integrated into the system. ~~Security awareness~~Role-based security and privacy training programs can ensure that individuals having 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 ensures that important security and privacy considerations are addressed early in the system ~~development~~ 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 risk management strategy of the organization. Because the development life cycle of a system involves multiple organizations, including, for example, external suppliers, developers, integrators, and service providers, it is important to recognize that acquisition and supply chain risk management functions and controls play a significant role in the overall effective management of the system during that life cycle.

Related Controls: AT-3, PL-8, PM-7, SA-4, SA-5, SA-8, SA-11, SA-12, SA-15, SA-17, SA-18, SA-22.

Control Enhancements:

(1) SYSTEM DEVELOPMENT LIFE CYCLE | MANAGE DEVELOPMENT ENVIRONMENT

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

Supplemental Guidance: None.

Related Controls: CM-2, CM-4, RA-3, SA-4.

(2) SYSTEM DEVELOPMENT LIFE CYCLE | USE OF LIVE DATA

(a) Approve, document, and control the use of live data in development, test, and integration environments for the system, system component, or system service; and

(b) Ensure development, test, and integration environments for the system, system component, or system service are protected at the same impact or classification level as any live data used.

Supplemental Guidance: Live data is also referred to as operational data. The use of live data in preproduction environments can result in significant risk to organizations. ~~organizational risk management and information~~Organizations can minimize such risk by using test or dummy data during the design, development, and testing of systems, system components, and system services.

Related Controls: RA-3.

(3) SYSTEM DEVELOPMENT LIFE CYCLE | TECHNOLOGY REFRESH

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

Supplemental Guidance: Technology refresh planning may encompass hardware, software, firmware, processes, personnel skill sets, suppliers, service providers, and facilities. The use of obsolete or nearing obsolete technology may increase security ~~strategies. Related controls: AT-3, PM-7, SA-8~~and privacy risks associated with, for example, unsupported components, components unable to implement security or privacy requirements, counterfeit or re-purposed components, slow or inoperable components, components from untrusted sources, inadvertent personnel error, or increased complexity.

Related Controls: None.

References: NIST Special Publications 800-30, 800-37, 800-64.

SA-4 ACQUISITION PROCESS

Control: Include the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the system, system component, or system service ~~in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs~~:

a. Security and privacy functional requirements;

b. ~~Security strength~~Strength of mechanism requirements;

c. Security and privacy assurance requirements;

d. Security ~~related~~ and privacy documentation requirements;

e. Requirements for protecting security ~~related~~ and privacy documentation;

f. Description of the system development environment and environment in which the system is intended to operate;

g. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; and

~~g.~~h. Acceptance criteria.

Supplemental Guidance: System components are discrete, identifiable information technology assets ~~(e.g.,~~including, for example, hardware, software, or firmware. These components represent the building blocks of a system. System components typically consist of commercial information technology products. Security and privacy functional requirements include security and privacy capabilities, ~~security~~ functions, and ~~security~~ mechanisms. ~~Security~~ Strength requirements associated with such capabilities, functions, and mechanisms include degree of correctness, completeness, resistance to ~~direct attack~~tampering or bypass, and resistance to ~~tampering or bypass.~~direct attack. Security and privacy assurance requirements include development processes, procedures, practices, and methodologies; and the evidence from development and assessment activities providing grounds for confidence that the required security and privacy functionality is implemented and possesses the required ~~security~~ strength ~~has been achieved.~~of mechanism. Security and privacy documentation requirements address all phases of the system development life cycle.

Security ~~functionality, assurance,~~ and ~~documentation~~privacy requirements are expressed in terms of security and privacy controls and control enhancements that have been selected through the tailoring process. The tailoring process includes, for example, the specification of parameter values using assignment and selection statements and ~~the specification of~~ platform dependencies and implementation information. Security and privacy documentation provides user and administrator guidance regarding the implementation and operation of security and privacy controls. The level of detail required in ~~security~~such documentation is based on the security categorization or classification level of the system and the degree to which organizations depend on the stated security or privacy capabilities, functions, or mechanisms to meet overall risk response expectations ~~(as defined in the organizational risk management strategy).~~ Security and privacy requirements can include ~~organizationally~~ mandated configuration settings specifying allowed functions, ports, protocols, and services. Acceptance criteria for systems, system components, and system services are defined in the same manner as such criteria for any organizational acquisition or procurement. ~~The Federal Acquisition Regulation (FAR) Section 7.103 contains information security requirements from FISMA.~~

Related Controls: CM-6, CM-8, PS-7, SA-3, SA-5, SA-8, SA-11, SA-12, SA-15, SA-16, SA-17, SA-21.

Control Enhancements:

(1) ACQUISITION PROCESS | FUNCTIONAL PROPERTIES OF ~~*SECURITY*~~ 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.

Supplemental Guidance: 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.

Related Controls: None.

(2) ACQUISITION PROCESS | DESIGN AND IMPLEMENTATION INFORMATION FOR ~~*SECURITY*~~ CONTROLS

Require the developer of the system, system component, or system service to provide design and implementation information for the selected 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*].

Supplemental Guidance: Organizations may require different levels of detail in design and implementation documentation for controls implemented in organizational systems, system components, or system services based on mission and business requirements; requirements for trustworthiness and resiliency; 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 ~~with particular emphasis on software and firmware (but not excluding hardware)~~ and the interfaces between modules providing security-relevant functionality. Design and implementation documentation may include information such as 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.

Related Controls: None.

(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 [*Assignment: organization-defined ~~state-of-the-practice system/security~~systems engineering methods; [Selection (one or more): systems security engineering methods; privacy engineering methods]; software development methods; testing, evaluation, assessment, verification, and validation ~~techniques,~~methods; and quality control processes*].

Supplemental Guidance: Following a ~~well-defined~~ system development life cycle that includes state-of-the-practice software development methods, systems~~/security~~ engineering methods, systems security and privacy engineering methods, and quality control processes~~, and testing, evaluation, and validation techniques~~ 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.

Related Controls: None.

(4) ACQUISITION PROCESS | ASSIGNMENT OF COMPONENTS TO SYSTEMS

[Withdrawn: Incorporated into CM-8(9)].

(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.

Supplemental Guidance: Security configurations include, for example, the U.S. Government Configuration Baseline (USGCB) and any limitations on functions, ports, protocols, and services. Security characteristics include, for example, requiring that default passwords have been changed.

Related Controls: None.

(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.

Supplemental Guidance: Commercial off-the-shelf IA or IA-enabled information technology products used to protect classified information by cryptographic means may be required to use NSA-approved key management.

Related Controls: SC-8, SC-12, SC-13.

(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.

Supplemental Guidance: None.

Related Controls: IA-7, SC-12, SC-13.

(8) ACQUISITION PROCESS | CONTINUOUS MONITORING PLAN FOR CONTROLS

Require the developer of the system, system component, or system service to produce a plan for continuous monitoring of security and privacy control effectiveness that contains the following: [*Assignment: organization-defined level of detail*].

Supplemental Guidance: The objective of continuous monitoring plans is to determine if the complete set of planned, required, and deployed security and privacy controls within the system, system component, or system service continue to be effective over time based on the inevitable changes that occur. Developer continuous monitoring plans include a sufficient level of detail such that the information can be incorporated into the continuous monitoring strategies and programs implemented by organizations.

Related Controls: CA-7.

(9) ACQUISITION PROCESS | FUNCTIONS, PORTS, PROTOCOLS, AND SERVICES IN USE

Require the developer of the system, system component, or system service to identify ~~early in the system development life cycle,~~ the functions, ports, protocols, and services intended for organizational use.

Supplemental Guidance: The identification of functions, ports, protocols, and services early in the system development life cycle, for example, during the initial requirements definition and design phases, allows organizations to influence the design of the system, system component, or system service. This early involvement in the system life cycle helps organizations to avoid or minimize the use of functions, ports, protocols, or services that pose unnecessarily high risks and understand the trade-offs involved in blocking specific ports, protocols, or services or when requiring system service providers to do so. Early identification of functions, ports, protocols, and services avoids costly retrofitting of controls after the system, ~~system~~ component, or system service has been implemented. SA-9 describes the requirements for external system services with organizations identifying which functions, ports, protocols, and services are provided from external sources.

Related Controls: CM-7, SA-9.

(10) ACQUISITION PROCESS | USE OF APPROVED PIV PRODUCTS

Employ only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational systems.

Supplemental Guidance: None.

Related Controls: IA-2, IA-8, PM-9.

References: ISO/IEC 15408; FIPS Publications 140-2, 201; NIST Special Publications 800-23, 800-35, 800-36, 800-37, 800-64, 800-70, 800-73, 800-137, 800-161; NIST Interagency Reports 7539, 7622, 7676, 7870, 8062.

SA-5 SYSTEM DOCUMENTATION

Control:

a. Obtain 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 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 takes [*Assignment: organization-defined actions*] in response;

d. Protect documentation as required, in accordance with the organizational risk management strategy; and

e. Distribute documentation to [*Assignment: organization-defined personnel or roles*].

Supplemental Guidance: This control helps organizational personnel understand the implementation and operation of security and privacy controls associated with systems, system components, and system services. Organizations consider establishing specific measures to determine the quality and completeness of the content provided. System documentation may be used, for example, to support the management of supply chain risk, incident response, and other functions. Personnel or roles requiring documentation may include, for example, system owners, system security officers, and system administrators. Attempts to obtain documentation may include, for example, directly contacting manufacturers or suppliers and conducting web-based searches. The inability to obtain needed documentation may occur, for example, due to the age of the system or component or lack of support from developers and contractors. In those situations, organizations may need to recreate selected documentation if such documentation is essential to the implementation or operation of the security and privacy controls. The level of protection provided for ~~selected information~~the system, component, or service documentation is commensurate with the security category or classification of the system. ~~For example, documentation associated with a key DoD weapons system or command and control system would typically require a higher level of protection than a routine administrative system.~~ Documentation that addresses system vulnerabilities may require an increased level of protection. Secure operation of the system, includes, for example, initially starting the system and resuming secure system operation after any lapse in system operation.

Related Controls: CM-4, CM-6, CM-7, CM-8, PL-2, PL-4, PL-8, PS-2, SA-3, SA-4, SA-9, SA-10, SA-11, SA-15, SA-16, SA-17, SI-12.

Control Enhancements:

(1) SYSTEM DOCUMENTATION | FUNCTIONAL PROPERTIES OF SECURITY CONTROLS
[Withdrawn: Incorporated into SA-4(1)].

(2) SYSTEM DOCUMENTATION | SECURITY-RELEVANT EXTERNAL SYSTEM INTERFACES
[Withdrawn: Incorporated into SA-4(2)].

(3) SYSTEM DOCUMENTATION | HIGH-LEVEL DESIGN
[Withdrawn: Incorporated into SA-4(2)].

(4) SYSTEM DOCUMENTATION | LOW-LEVEL DESIGN
[Withdrawn: Incorporated into SA-4(2)].

(5) SYSTEM DOCUMENTATION | SOURCE CODE
[Withdrawn: Incorporated into SA-4(2)].

References: None.

SA-6 SOFTWARE USAGE RESTRICTIONS

[Withdrawn: Incorporated into CM-10 and SI-7].

SA-7 USER-INSTALLED SOFTWARE

[Withdrawn: Incorporated into CM-11 and SI-7].

SA-8 SECURITY AND PRIVACY ENGINEERING PRINCIPLES

Control: Apply [*Assignment: organization-defined systems security engineering principles*] in the specification, design, development, implementation, and modification of the system and system components.

Supplemental Guidance: Organizations can apply systems security and privacy engineering principles ~~primarily~~ to new systems under development or to systems undergoing upgrades. For legacy 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. ~~Security engineering principles include, for example: (i) developing layered protections; (ii) establishing sound~~The application of systems security ~~policy,~~ and privacy engineering concepts and principles help to develop trustworthy, secure systems and system components and reduce the susceptibility of organizations to disruptions, hazards, threats, and creating privacy-related problems for individuals. Examples of these concepts and 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 ~~system~~ developers are trained on how to build secure software; tailoring security and privacy controls to meet organizational and operational needs; performing threat modeling to identify use cases, threat agents, attack vectors and ~~attack~~ patterns ~~as well as~~, design patterns, and compensating controls ~~and design patterns~~ needed to mitigate risk. Organizations that apply 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. Security engineering principles can also be used to protect against certain supply chain risks including, for example, incorporating tamper-resistant hardware into a design.

Related Controls: PL-8, PM-7, RA-2, RA-3, RA-9, SA-3, SA-4, SA-12, SA-15, SA-17, SA-20, SC-2, SC-3, SC-32, SC-39.

Control Enhancements: None.

References: FIPS Publications 199, 200; NIST Special Publications 800-53A, 800-60-1, 800-60-2, 800-64, 800-160; NIST Interagency Report 8062.

SA-9 EXTERNAL SYSTEM SERVICES

Control:

a. Require that providers of external system services comply with organizational security and privacy requirements and employ [*Assignment: organization-defined security* ~~*controls*~~] ~~in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;~~*and privacy controls*];

b. Define and document organizational oversight and user roles and responsibilities with regard to external system services; and

c. Employ [*Assignment: organization-defined processes, methods, and techniques*] to monitor security and privacy control compliance by external service providers on an ongoing basis.

Supplemental Guidance: External system services are those services that are implemented external to authorization boundaries of organizational systems. This includes services that are used by, but not a part of, organizational systems. ~~FISMA and OMB policy require that organizations using external service providers that are processing, storing, or transmitting federal information or operating information systems on behalf of the federal government ensure that such providers meet the same security requirements that federal agencies are required to meet.~~ Organizations

establish relationships with external service providers in a variety of ways including, for example, through business partnerships, contracts, interagency agreements, lines of business arrangements, licensing agreements, joint ventures, and supply chain exchanges. The responsibility for managing risks from the use of external system services remains with authorizing officials. For services external to organizations, a chain of trust requires that organizations establish and retain a level of confidence that each ~~participating~~ provider in the ~~potentially complex~~ consumer-provider relationship provides adequate protection for the services rendered. The extent and nature of this chain of trust varies based on the relationships between organizations and the external providers. Organizations document the basis for trust relationships so the relationships can be monitored over time. External system services documentation includes government, service providers, end user security roles and responsibilities, and service-level agreements. Service-level agreements define expectations of performance for implemented security and privacy controls; describe measurable outcomes, and identify remedies and response requirements for identified instances of noncompliance.

Related Controls: CA-3, CP-2, IR-4, IR-7, PL-10, PL-11, PS-7, SA-2, SA-4, SA-12.

Control Enhancements:

(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*].

Supplemental Guidance: Examples of information security services include the operation of security devices such as firewalls, or key management services; and incident monitoring, analysis and response. Risks assessed may include, for example, system-related, mission-related, privacy-related, or supply chain-related risks.

Related Controls: CA-6, RA-3.

(2) EXTERNAL SYSTEM SERVICES | IDENTIFICATION OF FUNCTIONS, PORTS, PROTOCOLS, AND SERVICES

Require providers of [*Assignment: organization-defined external system services*] to identify the functions, ports, protocols, and other services required for the use of such services.

Supplemental Guidance: Information from external service providers regarding the specific functions, ports, protocols, and services used in the provision of such services can be useful when the need arises to understand the trade-offs involved in restricting certain functions and services or blocking certain ports and protocols.

Related Controls: CM-6, CM-7.

(3) EXTERNAL SYSTEM SERVICES | ESTABLISH AND MAINTAIN TRUST RELATIONSHIP WITH PROVIDERS

Establish, document, and maintain trust relationships with external service providers based on [*Assignment: organization-defined security and privacy requirements, properties, factors, or conditions defining acceptable trust relationships*].

Supplemental Guidance: The degree of confidence that the risk from using external services is at an acceptable level depends on the trust that organizations place in the external providers, individually or in combination. Trust relationships can help organizations to gain increased levels of confidence that participating service providers are providing adequate protection for the services rendered. They can also be useful when conducting incident response or when planning for upgrades or obsolescence. Trust relationships can be complicated due to the number of potential entities participating in the consumer-provider interactions, subordinate relationships and levels of trust, and types of interactions between the parties. In some cases, the degree of trust is based on the level of control organizations can exert on external service providers regarding the controls necessary for the protection of the service, information, or individual privacy and the evidence brought forth as to the effectiveness of the implemented controls. The level of control is established by the terms and conditions of the contracts or service-level agreements. Extensive control may include negotiating contracts or agreements that specify security and privacy requirements for providers. Limited control may include using contracts or service-level agreements to obtain commodity services such as commercial

telecommunications services. ~~In other cases, levels of trust are based on factors that convince organizations that required security controls have been employed and that determinations of control effectiveness exist. For example, separately authorized external information system services provided to organizations through well-established business relationships may provide degrees of trust in such services within the tolerable risk range of the organizations using the services. External service providers may also outsource selected services to other external entities, making the trust relationship more difficult and complicated to manage. Depending on the nature of the services, organizations may find it very difficult to place significant trust in external providers. This is not due to any inherent untrustworthiness on the part of providers, but to the intrinsic level of risk in the services.~~.

Related Controls: SA-12.

(4) EXTERNAL SYSTEM SERVICES | CONSISTENT INTERESTS OF CONSUMERS AND PROVIDERS

~~employs~~Take [*Assignment: organization-defined ~~security safeguards~~actions*] to ~~ensure~~verify that the interests of [*Assignment: organization-defined external service providers*] are consistent with and reflect organizational interests.

Supplemental Guidance: 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 ~~correct~~required technical, ~~procedural~~management, or operational ~~safeguards~~controls in place may not be sufficient if the ~~service~~ providers that implement and ~~control~~manage those ~~safeguards~~controls are not operating in a manner consistent with the interests of the consuming organizations. The actions that organizations might take to address such concerns include, for example, requiring background checks for selected service provider personnel; examining ownership records; employing only trustworthy service providers, including providers with which organizations have had ~~positive experiences),~~successful trust relationships; and conducting routine periodic, unscheduled visits to service provider facilities.

Related Controls: None.

(5) EXTERNAL SYSTEM SERVICES | PROCESSING, STORAGE, AND SERVICE LOCATION

Restrict the location of [*Selection (one or more): information processing; information or data; system services*] to [*Assignment: organization-defined locations*] based on [*Assignment: organization-defined requirements or conditions*].

Supplemental Guidance: The location of information processing, information and data storage, or system services that are critical to organizations can have a direct impact on the ability of those organizations to successfully execute their missions and business functions. This occurs when external providers control the location of processing, storage, or services. The criteria that external providers use for the selection of processing, storage, or service locations may be different from the criteria organizations use. For example, organizations may desire that data or information storage locations are restricted to certain locations to help facilitate incident response activities in case of information security or privacy incidents. Such incident response activities including, for example, forensic analyses and after-the-fact investigations, may be adversely affected by the governing laws or protocols in the locations where processing and storage occur and/or the locations from which system services emanate.

Related Controls: SA-5, SA-12.

(6) EXTERNAL SYSTEM SERVICES | ORGANIZATION-CONTROLLED CRYPTOGRAPHIC KEYS

Maintain exclusive control of cryptographic keys.

Supplemental Guidance: Maintaining exclusive control of cryptographic keys in an external system prevents decryption of organizational data by external system staff. This enhancement can be implemented, for example, by encrypting and decrypting data inside the organization as data is sent to and received from the external system or through use of a component that permits encryption and decryption functions to be local to the external system, but allows the organization exclusive access to encryption keys.

Related Controls: SC-12, SC-13, SI-4.

(7) EXTERNAL SYSTEM SERVICES | ORGANIZATION-CONTROLLED INTEGRITY CHECKING

Provide the capability to check the integrity of organizational information while it resides in the external system.

Supplemental Guidance: Storage of organizational information in an external system could limit organizational visibility into the security status of its data. The ability for the organization to verify and validate the integrity of its stored data without transferring it out of the external system provides such visibility.

Related Controls: SI-7.

References: NIST Special Publications 800-35, 800-161.

SA-10 DEVELOPER CONFIGURATION MANAGEMENT

Control: 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*].

Supplemental Guidance: ~~This control also applies to organizations conducting internal information systems development and integration.~~ Organizations consider the quality and completeness of the configuration management activities conducted by developers as direct evidence of applying effective security ~~safeguards. Safeguards~~controls. Controls include, for example, protecting from unauthorized modification or destruction, the master copies of material used to generate security-relevant portions of the system hardware, software, and firmware. Maintaining the integrity of changes to the system, system component, or system service requires strict configuration control throughout the system development life cycle to track authorized changes and to prevent unauthorized changes. The configuration items that are placed under configuration management ~~(if existence/use is required by other security controls)~~ 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 ~~software/firmware~~ 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 phases of the system life cycle.

Related Controls: CM-2, CM-3, CM-4, CM-7, CM-9, SA-4, SA-5, SA-12, SI-2.

Control Enhancements:

(1) DEVELOPER CONFIGURATION MANAGEMENT | SOFTWARE AND FIRMWARE INTEGRITY VERIFICATION

Require the developer of the system, system component, or system service to enable integrity verification of software and firmware components.

Supplemental Guidance: This control enhancement allows organizations to detect unauthorized changes to software and firmware components ~~through the use of~~ using developer-provided tools, techniques, and mechanisms. Integrity checking mechanisms can also address counterfeiting of software and firmware components. Organizations verify the integrity of software and firmware components, for example, through secure one-way hashes provided by developers. Delivered software and firmware components also include any updates to such components.

Related Controls: SI-7.

(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.

Supplemental Guidance: Alternate configuration management processes may be required, for example, when organizations use commercial off-the-shelf information technology products. Alternate configuration management processes include organizational personnel that~~: (i) are responsible for reviewing/approving~~ review and approve proposed changes to systems, system components, and system services; and that conduct security and privacy impact analyses prior to the implementation of changes to systems, components, or services~~ (e.g., a configuration control board that considers security impacts of changes during development and includes representatives of both the organization and the developer, when applicable).~~

Related Controls: None.

(3) DEVELOPER CONFIGURATION MANAGEMENT | HARDWARE INTEGRITY VERIFICATION

Require the developer of the system, system component, or system service to enable integrity verification of hardware components.

Supplemental Guidance: This control enhancement allows organizations to detect unauthorized changes to hardware components using developer-provided tools, techniques, methods, and mechanisms. Organizations verify the integrity of hardware components, for example, with hard-to-copy labels and verifiable serial numbers provided by developers, and by requiring the implementation of anti-tamper technologies. Delivered hardware components also include updates to such components.

Related Controls: SI-7.

(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~~ and software/firmware,~~ source code, and object code with previous versions.

Supplemental Guidance: This control enhancement 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, and/or mechanisms provided by developers.

Related Controls: None.

(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 (hardware drawings and software/firmware code) describing the current version of security-relevant hardware, software, and firmware and the on-site master copy of the data for the current version.

Supplemental Guidance: This control enhancement addresses changes to hardware, software, and firmware components during initial development and during system life cycle updates. Maintaining the integrity between the master copies of security-relevant hardware, software, and firmware (including designs and source code) and the equivalent data in master copies on-site in operational environments is essential to ensure the availability of organizational systems supporting critical missions and business functions.

Related Controls: None.

(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.

Supplemental Guidance: The trusted distribution of security-relevant hardware, software, and firmware updates ensure that such updates are correct representations of the master copies maintained by the developer and have not been tampered with during distribution.

Related Controls: None.

References: FIPS Publications 140-2, 180-4, 202; NIST Special Publication 800-128.

SA-11 DEVELOPER ~~SECURITY~~ TESTING AND EVALUATION

Control: Require the developer of the system, system component, or system service, at all post-design phases of the system development life cycle, to:

a. Create and implement a security and privacy assessment plan;

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 ~~security~~ assessment plan and the results of the ~~security~~ testing and evaluation;

d. Implement a verifiable flaw remediation process; and

e. Correct flaws identified during ~~security~~ testing and evaluation.

Supplemental Guidance: Developmental ~~security~~ testing~~/evaluation occurs at all post-design phases of the system development life cycle. Such testing/~~ and evaluation confirms that the required security and privacy 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. These interconnections or changes ~~(e.g.,~~including, for example, upgrading or replacing applications, operating systems, and firmware, may adversely affect previously implemented security and privacy controls. This control provides additional types of ~~security~~ testing and evaluation that developers can conduct to reduce or eliminate potential flaws. Testing custom software applications may require approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Developers can use these analysis approaches in a variety of tools ~~(e.g., web-based application scanners, static analysis tools, binary analyzers)~~ and in source code reviews. Security and privacy assessment plans provide 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, and the types of artifacts produced during those processes. The depth of ~~security~~ testing and evaluation refers to the rigor and level of detail associated with the assessment process ~~(e.g., black box, gray box, or white box testing).~~ The *coverage* of ~~security~~ 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 documentation protection requirements.

Related Controls: CA-2, CA-7, CM-4, SA-3, SA-4, SA-5, SA-12, SA-15, SA-17, SI-2.

Control Enhancements:

(1) DEVELOPER ~~*SECURITY*~~ 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.

Supplemental Guidance: Static code analysis provides a technology and methodology for security reviews~~.~~ and may include, for example, checking for weaknesses in the code and checking for incorporation of libraries or other included code with known vulnerabilities or that are out-of-date and not supported. Such analysis can be used to identify ~~security~~

vulnerabilities and enforce ~~security~~secure coding practices. Static code analysis is most effective when used early in the development process, when each code change can be automatically scanned for potential weaknesses. Static analysis can provide clear remediation guidance along with defects to enable developers to fix such defects. Evidence of correct implementation of static analysis can include, for example, aggregate defect density for critical defect types; evidence that defects were inspected by developers or security professionals; and evidence that defects were remediated. An excessively 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.

Related Controls: None.

(2) DEVELOPER ~~*SECURITY*~~ 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 at [*Assignment: organization-defined breadth and depth*] during development and during the subsequent testing and evaluation of the ~~as-built~~ system, component, or service that:

(a) Uses [*Assignment: organization-defined information concerning impact, environment of operations, known or assumed threats, and acceptable risk levels*];

(b) Employs [*Assignment: organization-defined tools and methods*]; and

(c) Produces evidence that meets [*Assignment: organization-defined acceptance criteria*].

Supplemental Guidance: ~~Applications~~Systems, system components, and system services may deviate significantly from the functional and design specifications created during the requirements and design phases of the system development life cycle. Therefore, threat modeling and vulnerability analyses of those systems, system components, and system services prior to delivery are critical to the effective operation of those systems, components, and services. Threat modeling and vulnerability analyses at this phase of the system development life cycle ~~help to~~ ensure that design ~~or~~and implementation changes have been accounted for and ~~that any new~~ vulnerabilities created ~~as a result~~because of those changes have been reviewed and mitigated.

Related controls: PM-15, RA-3, RA-5.

(3) DEVELOPER ~~*SECURITY*~~ TESTING AND EVALUATION | INDEPENDENT VERIFICATION OF ASSESSMENT PLANS AND EVIDENCE

(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 ~~security~~ 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.

Supplemental Guidance: Independent agents have the necessary qualifications, including the expertise, skills, training, certifications, and experience, to verify the correct implementation of developer security and privacy assessment plans.

Related Controls: AT-3, RA-5.

(4) DEVELOPER ~~*SECURITY*~~ 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 [*Assignment: organization-defined processes, procedures, and/or techniques*].

Supplemental Guidance: Manual code reviews are usually reserved for the critical software and firmware components of systems. Such code reviews are ~~uniquely~~ effective ~~at~~in identifying weaknesses that require knowledge of the application's requirements or context which in most cases, are unavailable to automated analytic tools and techniques including static and dynamic analysis. Components benefiting from manual review include, for example, verifying access control matrices against application controls and reviewing more detailed aspects of cryptographic implementations and controls.

Related Controls: None.

(5) DEVELOPER ~~*SECURITY*~~ TESTING AND EVALUATION | PENETRATION TESTING ~~*/ ANALYSIS*~~

Require the developer of the system, system component, or system service to perform penetration testing at [*Assignment: organization-defined breadth and depth*] and with [*Assignment: organization-defined constraints*].

Supplemental Guidance: Penetration testing is an assessment methodology in which assessors, using all available information technology product or system documentation ~~(e.g., product/system design specifications, source code, and administrator/operator manuals)~~ and working under specific constraints, attempt to circumvent implemented security and privacy features of information technology products and systems. Useful information for assessors conducting penetration testing can include, for example, product and system design specifications, source code, and administrator and operator manuals. Penetration testing can include white-box, gray-box, or black box testing with associated analyses performed by skilled ~~security~~ professionals simulating adversary actions. The objective of penetration testing is to uncover the potential vulnerabilities in ~~information technology products and~~ systems, system components and services resulting from implementation errors, configuration faults, or other operational ~~deployment~~ weaknesses or deficiencies. Penetration tests can be performed in conjunction with automated and manual code reviews to provide greater levels of analysis than would ordinarily be possible.

Related Controls: CA-8.

(6) DEVELOPER ~~*SECURITY*~~ TESTING AND EVALUATION | ATTACK SURFACE REVIEWS

Require the developer of the system, system component, or system service to perform attack surface reviews.

Supplemental Guidance: Attack surfaces of systems and system components are exposed areas that make those systems more vulnerable to ~~cyber~~ attacks. This includes any accessible areas where weaknesses or deficiencies in ~~information systems (including~~ the hardware, software, and firmware components provide opportunities for adversaries to exploit vulnerabilities. Attack surface reviews ensure that developers analyze the design and implementation changes to systems and mitigate attack vectors generated as a result of the changes. Correction of identified flaws includes, for example, deprecation of unsafe functions.

Related Controls: None.

(7) DEVELOPER ~~*SECURITY*~~ 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 of ~~security~~ testing and evaluation provides complete coverage of required security and privacy controls at [*Assignment: organization-defined depth of testing and evaluation*].

Supplemental Guidance: Verifying that ~~security~~ testing and evaluation provides complete coverage of required security and privacy controls can be accomplished by a variety of analytic techniques ranging from informal to formal. Each of these techniques provides an increasing level of assurance corresponding to the degree of formality of the analysis. Rigorously demonstrating ~~security~~ control coverage at the highest levels of assurance can be provided using formal modeling and analysis techniques including correlation between control implementation and corresponding test cases.

Related Controls: None.

(8) DEVELOPER ~~*SECURITY*~~ 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.

Supplemental Guidance: Dynamic code analysis provides run-time verification of software programs, using tools capable of monitoring programs for memory corruption, user privilege issues, and other potential security problems. Dynamic code analysis employs run-time tools to ensure that security functionality performs in the way it was designed. A specialized type of dynamic analysis, known as fuzz testing, induces program failures by deliberately introducing malformed or random data into software programs. Fuzz testing strategies derive from the intended use of applications and the associated functional and design specifications for the applications. To understand the scope of dynamic code analysis and hence the assurance provided, organizations may also consider conducting code coverage analysis

(checking the degree to which the code has been tested using metrics such as percent of subroutines tested or percent of program statements called during execution of the test suite) and/or concordance analysis (checking for words that are out of place in software code such as non-English language words or derogatory terms).

Related Controls: None.

References: ISO/IEC 15408; NIST Special Publications 800-30, 800-53A, 800-154.

SA-12 SUPPLY CHAIN ~~PROTECTION~~RISK MANAGEMENT

Control: ~~The organization protects against supply chain threats to the information system, system component, or information system service by employing~~

a. Employ [*Assignment: organization-defined ~~security~~supply chain safeguards*] ~~as part of a comprehensive, defense-in-breadth information security strategy.~~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; and

b. Document the selected and implemented supply chain safeguards in [*Selection: security and privacy plans; supply chain risk management plan;* [*Assignment: organization-defined document*]].

Supplemental Guidance: ~~Information systems (~~Supply chain-related events including~~ system components that compose those systems) need to be protected throughout the system~~, for example, disruption, theft, insertion of counterfeits, insertion of malicious code, malicious development ~~life cycle (i.e., during design, development, manufacturing, packaging, assembly, distribution, system integration, operations, maintenance, and retirement). Protection of organizational information systems is accomplished through threat awareness, by the identification, management, and reduction of vulnerabilities at each phase of the life cycle and the use of complementary, mutually reinforcing strategies to respond to risk. Organizations consider implementing a standardized process to address supply chain risk with respect to information systems and system components, and to educate the acquisition workforce on threats, risk, and required security controls. Organizations use the acquisition/procurement processes to require supply chain entities to implement necessary security safeguards to: (i) reduce the likelihood of unauthorized modifications at each stage in the supply chain; and (ii) protect information systems and information system components, prior to taking~~practices, improper delivery ~~of such systems/components. This control enhancement also applies to information system services. Security safeguards include, for example: (i) security controls for development systems, development facilities, and external connections to development systems; (ii) vetting development personnel; and (iii) use of tamper-evident packaging during shipping/warehousing.~~practices, and use of defective components, can adversely impact the confidentiality, integrity, or availability of information processed, stored, or transmitted by a system. Such events can also adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. Supply chain-related events may be unintentional or malicious and occur at any point during the system life cycle. Managing supply chain risks involves gaining visibility and understanding of the processes and procedures used to protect the system, system component, or system service throughout the system life cycle. This allows organizations to make appropriate acquisition decisions and to identify appropriate mitigation strategies. A supply chain risk management plan includes, for example, an unambiguous expression of the supply chain risk tolerance for the system, acceptable supply chain risk mitigation strategies or controls, a description of and justification for supply chain protection measures taken, a process for consistently evaluating and monitoring supply chain risk, approaches for implementing and communicating the supply chain risk management plan, and associated roles and responsibilities.

Related Controls: AT-3, CM-8, IR-4, IR-6, MA-2, MA-6, PE-3, PE-16, PL-8, PM-31, RA-3, RA-7, RA-9, SA-2, SA-3, SA-4, SA-5, SA-8, SA-9, SA-10, SA-15, SA-18, SA-19, SC-7, SC-29, SC-30, SC-38, SI-7.

Control Enhancements:

(1) SUPPLY CHAIN RISK MANAGEMENT~~PROTECTION~~ | ACQUISITION STRATEGIES, TOOLS, AND METHODS

Employ [*Assignment: organization-defined acquisition strategies, contract tools, and procurement methods*] ~~to protect against, identify, and mitigate supply chain risks.z For the purchase of the information system, system component, or information system sercice from supliers.~~

Supplemental Guidance: The use of the acquisition process early in the system development life cycle provides an important vehicle to protect the supply chain. ~~Organizations use available all-source intelligence analysis to inform the tailoring of acquisition strategies, tools, and methods.~~ There are many useful tools and techniques available including, for example, obscuring the end use of a system or system component, using blind or filtered buys, requiring tamper-evident packaging, or using trusted or controlled distribution. The results from a supply chain risk assessment can inform which strategies, tools, and methods are most applicable to the situation. Tools and techniques may provide protections against the insertion of counterfeits, tampering, theft, unauthorized production, insertion of malicious software, as well as poor manufacturing and development practices throughout the system development life cycle. Organizations also consider creating incentives for suppliers who implement security and privacy controls; promote transparency into their organizational processes and security and privacy practices; provide additional vetting of the processes and practices of subordinate suppliers, critical system components, and services; restrict purchases from specific suppliers; and provide contract language that addresses the prohibition of tainted or counterfeit components. Finally, organizations consider providing training, education, and awareness programs for organizational personnel regarding supply chain risk, available mitigation strategies, and when they should be used. Methods for reviewing and protecting development plans, evidence, and documentation are commensurate with the security category or classification level of the information system. Contracts may specify documentation protection requirements.

(2) SUPPLY CHAIN RISK MANAGEMENT~~PROTECTION~~ | SUPPLIER REVIEWS

~~**The organization conducts a supplier review prior to entering into a contractual agreement to acquire the information**~~

Review the supply chain-related risks associated with suppliers or contractors and the system, system component, or ~~information~~ system service they provide [*Assignment: organization-defined frequency*].

Supplemental Guidance: A review of supplier risk may include, for example~~: (i) analysis of supplier~~, the ability of the supplier to effectively assess or vet any subordinate second-tier and third-tier suppliers and contractors. These reviews may be conducted by the organization or by an independent third party. The reviews consider documented processes ~~used to design, develop, test, implement, verify, deliver, and support~~, documented controls, publicly available information ~~systems, system components, and~~ related to the supplier or contractor, and all-source intelligence where possible. The organization can use open-source information ~~system services; and (ii) assessment of supplier training~~ to monitor for indications of stolen CUI, poor development and ~~experience in developing systems, components, or services~~quality control practices, information spillage, or counterfeits. In some cases, it may be appropriate to share review results with ~~the required security capability. These reviews provide~~other organizations in accordance with ~~increased levels of visibility into supplier activities during the system development life cycle to promote more effective~~ any applicable inter-organizational agreements or contracts. ~~Supplier reviews can also help to determine whether primary suppliers have security safeguards in place and a practice for vetting subordinate suppliers, for example, second- and third-tier suppliers, and any subcontractors.~~

Related Controls: None.

(3) SUPPLY CHAIN RISK MANAGEMENT ~~*SUPPLY CHAIN PROTECTION*~~ | TRUSTED SHIPPING AND WAREHOUSING

[Withdrawn: Incorporated into SA-12(1)].

(4) SUPPLY CHAIN ~~*PROTECTION*~~RISK MANAGEMENT | DIVERSITY OF SUPPLIERS

[Withdrawn: Incorporated into SA-12(13)].

(5) SUPPLY CHAIN ~~*PROTECTION*~~RISK MANAGEMENT | LIMITATION OF HARM

Employ [*Assignment: organization-defined ~~security~~ safeguards*] to limit harm from potential adversaries identifying and targeting the organizational supply chain.

Supplemental Guidance: ~~Supply chain risk is part of the advanced persistent threat (APT). Security safeguards and countermeasures~~Safeguards that can be implemented to reduce the probability of adversaries successfully identifying and targeting the supply chain include, for example, avoiding the purchase of custom or non-standardized configurations~~ to reduce the risk of acquiring information systems, components, or products that have been corrupted via supply chain actions targeted at specific organizations~~; employing a diverse set of suppliers ~~to limit the potential harm from any given supplier in the supply chain;~~ ; employing approved vendor lists with standing reputations in industry; using procurement carve outs that provide exclusions to commitments or obligations; and designing the system to include diversity of materials, components, and paths. In addition, organizations consider minimizing the time between purchase decisions and required delivery to limit the opportunities for adversaries to corrupt system components.

Related Controls: None.

(6) SUPPLY CHAIN ~~*PROTECTION*~~RISK MANAGEMENT | MINIMIZING PROCUREMENT TIME

[Withdrawn: Incorporated into SA-12(1)].

(7) SUPPLY CHAIN ~~*PROTECTION*~~RISK MANAGEMENT | ASSESSMENTS PRIOR TO SELECTION, ACCEPTANCE, AND UPDATE

Assess the system, system component, or system service prior to selection, acceptance, modification, or update.

Supplemental Guidance: ~~Assessments include, for example, testing, evaluations, reviews, and analyses. Independent, third-party entities or~~ Organizational personnel or independent, external entities conduct assessments of systems, components, products, tools, and services~~. Organizations conduct assessments~~ to uncover unintentional ~~vulnerabilities~~ and intentional vulnerabilities~~ including, for example,~~, evidence of tampering, or evidence of non-compliance with supply chain controls. These include, for example, malicious code, malicious processes, defective software, and counterfeits. Assessments can include, for example, visual or physical inspection; evaluations; design proposal reviews; static ~~analyses,~~and dynamic analyses; visual, x-ray, or magnetic particle inspections; simulations; white, gray, and black box testing; fuzz testing; stress testing; and penetration testing~~, and ensuring~~. Organizations can also ensure that the components or services are genuine by using, for example, tags, cryptographic hash verifications, or digital signatures. Evidence generated during security assessments is documented for follow-on actions carried out by organizations.

Related Controls: CA-2, CA-8, RA-5, SA-11, SI-7.

(8) SUPPLY CHAIN ~~*PROTECTION*~~RISK MANAGEMENT | USE OF ALL-SOURCE INTELLIGENCE

Use all-source intelligence to assist in the analysis of ~~suppliers and potential suppliers of the information system, system component, or information system service~~supply chain risk.

Supplemental Guidance: Organizations employ all-source intelligence to inform engineering, acquisition, and supply chain risk management decisions. All-source intelligence consists of ~~intelligence products and/or organizations and activities that incorporate~~information derived from all available sources ~~of information, most frequently,~~ including, for example, publicly available or open-source information; human intelligence; signals intelligence; imagery intelligence; and measurement and signature intelligence ~~and open-source data in the production of finished intelligence.~~. This information is used to analyze the risk of intentional and unintentional vulnerabilities from development, manufacturing, and delivery processes, people, and the environment. This review 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.

Related Controls: None.

(9) SUPPLY CHAIN ~~*PROTECTION*~~RISK MANAGEMENT | OPERATIONS SECURITY

Employ [*Assignment: organization-defined Operations Security (OPSEC) safeguards*] ~~in accordance with classification guides~~ to protect supply chain-related information for the system, system component, or system service.

Supplemental Guidance: Supply chain information includes, for example, user identities; uses for systems, system components, and system services; supplier identities; supplier processes; security requirements; design specifications; testing and evaluation results; and system and component configurations. This control enhancement expands the scope of OPSEC to include suppliers and potential suppliers. OPSEC is a process of identifying critical information and subsequently analyzing friendly actions attendant to operations and other activities to identify those actions that can be observed by potential adversaries; determine indicators that potential adversaries might obtain that could be interpreted or pieced together to derive information in sufficient time to cause harm to organizations; implement safeguards or countermeasures to eliminate or reduce to an acceptable level, exploitable vulnerabilities; and finally, consider how aggregated information may compromise the confidentiality of users or the specific uses of the supply chain. OPSEC may require organizations to withhold specific mission/business information from suppliers and may include the use of intermediaries to hide the end use, or users of systems, system components, or system services.

Related Controls: SC-38.

(10) SUPPLY CHAIN ~~*PROTECTION*~~RISK MANAGEMENT | VALIDATE AS GENUINE AND NOT ALTERED

Employ [*Assignment: organization-defined security safeguards*] to validate that the system or system component received is genuine and has not been altered.

Supplemental Guidance: For ~~some~~ many systems and system components, especially hardware, there are technical means to determine if the ~~components~~items are genuine or have been altered~~. Security safeguards used to validate the authenticity of information systems and information system components include~~, including, for example, optical and nanotechnology tagging; physically unclonable functions; side-channel analysis~~. For hardware, detailed bill of material information can highlight the elements with embedded logic complete with component ;~~ and ~~production location.~~

visible anti-tamper stickers and labels. Safeguards can also include monitoring for out of specification performance, which can be an indicator of tampering or counterfeits. Suppliers and contractors may have processes for validating that a system or component is genuine and has not been altered, and for replacing a suspect system or component, which the organization may leverage. Some indications of tampering may be visible and addressable before accepting delivery including, for example, broken seals, inconsistent packaging, and incorrect labels. The organization may consider providing training to appropriate personnel on how to identify suspicious system or component deliveries. When a system or component is suspected of being altered or counterfeit, the organization considers notifying the supplier, contractor, or original equipment manufacturer who may be able to replace the item or provide a forensic capability to determine the origin of the counterfeit or altered item.

Related Controls: SA-19.

(11) SUPPLY CHAIN RISK MANAGEMENT | PENETRATION TESTING AND ANALYSIS

Employ [*Selection (one or more): organizational analysis, independent third-party analysis, organizational penetration testing, independent third-party penetration testing*] of [*Assignment: organization-defined supply chain elements, processes, and actors*] associated with the *system, system component, or system service*.

Supplemental Guidance: This control enhancement addresses analysis or testing of the supply chain~~, not just delivered items. Supply chain elements are information technology products or product~~. It also considers the relationships or linkages between entities and procedures within the supply chain including, for example, development and delivery. Supply chain elements include system components that contain programmable logic and that are critically important to ~~information~~ system functions. Supply chain processes include, for example, hardware, software, and firmware development processes; shipping and handling procedures; personnel and physical security programs; configuration management tools, techniques, and measures to maintain provenance; and programs, processes, or procedures associated with the production and distribution of supply chain elements. Supply chain actors are individuals with specific

roles and responsibilities in the supply chain. The evidence generated and collected during analyses and testing of supply chain elements, processes, and actors is documented and used to inform organizational risk management activities and decisions.

Related Controls: RA-5.

~~(11)~~(12) SUPPLY CHAIN ~~PROTECTION | INTER-ORGANIZATIONAL~~ RISK MANAGEMENT | NOTIFICATION AGREEMENTS

Establish agreements and procedures with entities involved in the supply chain for the system, system component, or system service for the [*Selection (one or more): notification of supply chain compromises; results of assessments or audits; [Assignment: organization-defined information*]].

Supplemental Guidance: The establishment of agreements and procedures provides for formal communications among supply chain entities. Early notification of compromises in the supply chain that can potentially adversely affect or have adversely affected organizational systems, including critical system components, is essential for organizations to effectively respond to such incidents. The results of assessments or audits may include open-source information that contributed to a decision or result and could be used to help the supply chain entity resolve a concern or improve its processes.

Related Controls: IR-8.

(13) SUPPLY CHAIN ~~PROTECTION~~ RISK MANAGEMENT | CRITICAL SYSTEM COMPONENTS

~~*SUPPLY CHAIN PROTECTION | CRITICAL INFORMATION SYSTEM COMPONENTS*~~

~~**The organization employs [*Assignment: organization-defined security safeguards*] to ensure an adequate supply of [*Assignment: organization-defined critical information system components*].**~~

~~Supplemental Guidance: Adversaries can attempt to impede organizational operations by disrupting the supply of critical information system components or corrupting supplier operations. Safeguards to ensure adequate supplies of critical information system components include, for example: (i) the use multiple suppliers throughout the supply chain for the identified critical components; and (ii) stockpiling of spare components to ensure operation during mission-critical times~~

[Withdrawn: Incorporated into MA-6 and RA-9].

~~(12)~~(14) SUPPLY CHAIN RISK MANAGEMENT | IDENTITY AND TRACEABILITY

Establish and maintain unique identification of [*Assignment: organization-defined supply chain elements, processes, and ~~actors~~*] ~~for~~*personnel*] associated with the ~~information~~[*Assignment: organization-defined system, critical system ~~component, or information system service.~~components*].

Supplemental Guidance: Knowing who and what is in the supply chains of organizations is critical to gaining visibility into what is happening within such supply chains. It is also important for monitoring and identifying high-risk events and activities. Without reasonable visibility and traceability into supply chains (i.e., elements, processes, and ~~actors~~personnel), it is very difficult for organizations to understand, and therefore manage risk, and ultimately reduce the likelihood of or susceptibility to adverse events. ~~Uniquely identifying acquirer and integrator roles, organizations, personnel, mission and element processes, testing and evaluation procedures, delivery mechanisms, support mechanisms, communications/delivery paths, and disposal/final disposition activities as well as the components and tools used,~~Supply chain elements are systems or system components that contain programmable logic and that are critically important to system functions. Supply chain processes include, for example, hardware, software, and firmware development processes; shipping and handling procedures; personnel and physical security programs; configuration management tools, techniques, and measures to maintain provenance; or other programs, processes, or procedures associated with the production and distribution of supply chain elements. Supply chain personnel are individuals in the supply chain with specific roles and responsibilities related to, for example, the secure development, delivery, maintenance, and disposal of a system or system component. Tracking the unique identifiers of supply chain elements, processes, and personnel establishes a foundational identity structure for assessment of supply chain activities~~. For example, labeling (~~ and for the establishment and maintenance of provenance. For example, supply chain elements may be labeled using serial numbers~~) and tagging (~~ or tagged using radio-frequency identification tags~~) individual supply chain

~~elements including software packages, modules, and hardware devices, and processes associated with those elements can be used for this purpose.~~. These labels and tags can help provide the organization better visibility into the provenance of that element. Identification methods are sufficient to support ~~the provenance~~a forensic investigation in the event of a supply chain ~~issue~~compromise or ~~adverse supply chain~~ event.

Related Controls: CM-8, IA-2, IA-8.

~~(13)~~(15) SUPPLY CHAIN ~~PROTECTION~~RISK MANAGEMENT | PROCESSES TO ADDRESS WEAKNESSES OR DEFICIENCIES

Establish a process or processes to address weaknesses or deficiencies in supply chain elements ~~identified during~~in coordination with [*Assignment: organization-defined supply chain personnel*].

Supplemental Guidance: Supply chain elements are system or system components that contain programmable logic and that are critically important to system functions. Supply chain processes include, for example, hardware, software, and firmware development processes; shipping and handling procedures; personnel and physical security programs; configuration management tools, techniques, and measures to maintain provenance; or other programs, processes, or procedures associated with the production and distribution of supply chain elements. Supply chain personnel are individuals with specific roles and responsibilities in the supply chain. The evidence generated during the independent or organizational assessments of designated supply chain elements may be used to improve the supply chain processes and inform the organization's supply chain risk management process. The evidence can also be leveraged in follow-on assessments. Evidence and other related documentation may be shared in accordance with organizational agreements

Related Controls: None.

(16) SUPPLY CHAIN RISK MANAGEMENT | PROVENANCE

Document, monitor, and maintain valid provenance of [*Assignment: organization-defined systems, system components, and associated data*].

Supplemental Guidance: Every system and system component has a point of origin and may be changed throughout its existence. Provenance is the chronology of the origin, development, ownership, location, and changes to a system or system component and associated data. It may also include personnel and processes used to interact with or make modifications to the system, component, or associated data. Organizations consider developing procedures for allocating responsibilities for the creation, maintenance, and monitoring of provenance for systems and components; transferring provenance documentation and responsibility between organizations; and preventing and monitoring for unauthorized changes to the provenance records. Organizations consider developing methods to document, monitor, and maintain valid provenance baselines for systems, system components, and related data. Such actions help track, assess, and document changes to the provenance, including changes in supply chain elements or configuration, and ensure non-repudiation of provenance information and the provenance change records.

Related Controls: RA-9.

References: FIPS Publications 140-2, 180-4, 186-4, 202; NIST Special Publications 800-30, 800-161; NIST Interagency Report 7622.

SA-13 TRUSTWORTHINESS

~~Control: The organization:~~

~~c. Describes the trustworthiness required in the [*Assignment: organization-defined information system, information system component, or information system service*] supporting its critical missions/business functions; and~~

~~d. Implements [*Assignment: organization-defined assurance overlay*] to achieve such trustworthiness.~~

Supplemental Guidance: This control helps organizations to make explicit trustworthiness decisions when designing, developing, and implementing information systems that are needed to conduct critical organizational missions/business functions. Trustworthiness is a characteristic/property of an information system that expresses the degree to which the system can be expected to preserve the confidentiality, integrity, and availability of the information it processes, stores, or transmits. Trustworthy information systems are systems that are capable of being trusted to operate within defined levels of *risk* despite the environmental disruptions, human errors, and purposeful attacks that are expected to occur in the specified environments of operation. Trustworthy systems are important to mission/business success. Two factors affecting the trustworthiness of information systems include: (i) security functionality (i.e., the security features, functions, and/or mechanisms employed within the system and its environment of operation); and (ii) security assurance (i.e., the grounds for confidence that the security functionality is effective in its application). Developers, implementers, operators, and maintainers of organizational information systems can increase the level of assurance (and trustworthiness), for example, by employing well-defined security policy models, structured and rigorous hardware, software, and firmware development techniques, sound system/security engineering principles, and secure configuration settings (defined by a set of assurance-related security controls in Appendix E).

Assurance is also based on the assessment of evidence produced during the system development life cycle. Critical missions/business functions are supported by high-impact systems and the associated assurance requirements for such systems. The additional assurance controls in Table E-4 in Appendix E (designated as optional) can be used to develop and implement high-assurance solutions for specific information systems and system components using the concept of overlays described in Appendix I. Organizations select assurance overlays that have been developed, validated, and approved for community adoption (e.g., cross-organization, governmentwide), limiting the development of such overlays on an organization-by-organization basis. Organizations can conduct criticality analyses as described in SA-14, to determine the information systems, system components, or information system services that require high-assurance solutions. Trustworthiness requirements and assurance overlays can be described in the security plans for organizational information systems. Related controls: RA-2, SA-4,

[Withdrawn: Incorporated into SA-8, SA-14, SC-3.].

SA-14 CRITICALITY ANALYSIS

The organization identifies critical information system components and functions by performing a criticality analysis for [*Assignment: organization-defined information systems, information system components, or information system services*] at [*Assignment: organization-defined decision points in the system development life cycle*].

Supplemental Guidance: Criticality analysis is a key tenet of supply chain risk management and informs the prioritization of supply chain protection activities such as attack surface reduction, use of all-source intelligence, and tailored acquisition strategies. Information system engineers can conduct an end-to-end functional decomposition of an information system to identify mission-critical functions and components. The functional decomposition includes the identification of core 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 beyond the information system boundary. Information system components that allow for unmediated access to critical components or functions are considered critical due to the inherent vulnerabilities such components create. Criticality is assessed in terms of the impact of the function or component failure on the ability of the component to complete the organizational missions supported by the information system. A criticality analysis is performed whenever an architecture or design is being developed or modified, including upgrades. Related controls: CP-2, PL-2, PL-8, PM-1, SA-8, SA-12, SA-13, SA-15, SA-20.

Control Enhancements: None.

CRITICALITY ANALYSIS | CRITICAL COMPONENTS WITH NO VIABLE ALTERNATIVE SOURCING

[Withdrawn: Incorporated into SA-20RA-9].

SA-15 DEVELOPMENT PROCESS, STANDARDS, AND TOOLS

Control:

a. Require the developer of the system, system component, or system service to follow a documented development process that:

   1. Explicitly addresses security 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 [*Assignment: organization-defined security and privacy requirements*].

Supplemental Guidance: Development tools include, for example, programming languages and computer-aided design systems. Reviews of development processes can include, for example, the use of maturity models to determine the potential effectiveness of such processes. Maintaining the integrity of changes to tools and processes facilitates effective supply chain risk assessment and mitigation. Such integrity requires ~~robust~~ configuration control throughout the ~~life cycle (including design,~~system development~~, transport, delivery, integration, and maintenance)~~ life cycle to track authorized changes and to prevent unauthorized changes.

Related Controls: MA-6, SA-3, SA-4, SA-8, SA-11, SA-12.

Control Enhancements:

(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 smilestones*]; *upon delivery*].

Supplemental Guidance: Organizations use quality metrics to establish ~~minimum~~ acceptable levels of ~~information~~ system quality. Metrics may include quality gates which are collections of completion criteria or sufficiency standards representing the satisfactory execution of ~~particular~~specific phases of the system development project. A quality gate, for example, may require the elimination of all compiler warnings or ~~an explicit~~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. These metrics can include defining the severity thresholds of vulnerabilities, for example, requiring no known vulnerabilities in the delivered system with a Common Vulnerability Scoring System (CVSS) severity of Medium or High.

Related Controls: None.

(2) DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | SECURITY TRACKING TOOLS

Require the developer of the system, system component, or system service to select and employ a security tracking tool for use during the development process.

Supplemental Guidance: System development teams select and deploy security tracking tools, including, for example, vulnerability/work item tracking systems that facilitate assignment, sorting, filtering, and tracking of completed work items or tasks associated with system development processes.

Related Controls: SA-11.

(3) DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | CRITICALITY ANALYSIS

Require the developer of the system, system component, or system service to perform a criticality analysis at [*Assignment: organization-defined breadth/depth*] and at [*Assignment: organization-defined decision points in the system development life cycle*].

Supplemental Guidance: This control enhancement provides developer input to the criticality analysis performed by organizations ~~in SA-14~~. Developer input is essential to such analysis because organizations may not have access to detailed design documentation for system components that are developed as commercial off-the-shelf products. Such design documentation includes, for example, functional specifications, high-level designs, low-level designs, and source code and hardware schematics. Criticality analysis is important for organizational systems that are designated as high value assets. Such assets can be moderate- or high-impact systems due to the potential for serious, severe, or catastrophic adverse impacts on organizational missions or business functions.

Related Controls: RA-9.

(4) DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | THREAT MODELING AND VULNERABILITY ANALYSIS

~~**The organization requires that developers perform threat modeling and a vulnerability analysis for the information system at [*Assignment: organization-defined breadth/depth*] that:**~~

~~**Uses [*Assignment: organization-defined information concerning impact, environment of operations, known or assumed threats, and acceptable risk levels*];**~~

~~**Employs [*Assignment: organization-defined tools and methods*]; andProduces evidence that meets [*Assignment: organization-defined acceptance criteria*].**~~

~~Supplemental Guidance: Related control: SA-4.~~

[Withdrawn: Incorporated into SA-11(2)].

(5) DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | ATTACK SURFACE REDUCTION

Require the developer of the system, system component, or system service to reduce attack surfaces to [*Assignment: organization-defined thresholds*].

Supplemental Guidance: Attack surface reduction is closely aligned with developer threat and vulnerability analyses and system architecture and design. Attack surface reduction is a means of reducing risk to organizations by giving attackers less opportunity to exploit weaknesses or deficiencies (i.e., potential vulnerabilities) within systems, system components, and system services. Attack surface reduction includes, for example, employing the concept of layered defenses; applying the principles of least privilege and least functionality ~~(i.e., restricting ports, protocols, functions, and services);~~ deprecating unsafe functions; applying secure software development practices including, for example, reducing the amount of code executing and reducing entry points available to unauthorized users; and eliminating application programming interfaces (APIs) that are vulnerable to ~~cyber~~ attacks.

Related Controls: AC-6, CM-7, RA-3.

(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.

Supplemental Guidance: Developers of systems, system components, and system services consider the effectiveness and efficiency of their current development processes for meeting quality objectives and for addressing the security and privacy capabilities in current threat environments.

Related Controls: None.

(7) DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | AUTOMATED VULNERABILITY ANALYSIS

Require the developer of the system, system component, or system service 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*].

Supplemental Guidance: None.

Related Controls: RA-5, SA-11.

(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.

Supplemental Guidance: 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. ~~Authoritative~~ Vulnerability information is available from a variety of public and private sector sources including, for example, the NIST National Vulnerability Database.

Related Controls: None.

(9) DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | USE OF LIVE DATA

~~**The organization approves, documents, and controls the use of live data in development and test environments for the information system, system component, or information system service.**~~

~~Supplemental Guidance: The use of live data in preproduction environments can result in significant risk to organizations. Organizations can minimize such risk by using test or dummy data during the development and testing of information systems, information system components, and information system services.~~

[Withdrawn: Incorporated into SA-3(2)].

(10) DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | INCIDENT RESPONSE PLAN

Require the developer of the system, system component, or system service to provide, implement, and test an incident response plan.

Supplemental Guidance: The incident response plan provided by developers of systems, system components, and system services may be incorporated into organizational incident response plans. This information provides the type of incident response information that is not readily available to organizations. Such information may be extremely helpful, for example, when organizations respond to vulnerabilities in commercial off-the-shelf products.

Related Controls: IR-8.

(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 be released or delivered together with the corresponding evidence supporting the final security and privacy review.

Supplemental Guidance: Archiving system or system components requires the developer to retain key development artifacts including, for example, hardware specifications, source code, object code, and any relevant documentation from the development process that can provide a readily available configuration baseline ~~of information that can be helpful during information system~~/for system and component upgrades or modifications.

Related Controls: None.

References: None.

SA-16 DEVELOPER-PROVIDED TRAINING

Control: Require the developer of the system, system component, or system service to provide [*Assignment: organization-defined training*] on the correct use and operation of the implemented security and privacy functions, controls, and/or mechanisms.

Supplemental Guidance: This control applies to external and internal (in-house) developers. Training of personnel is an essential element to ensure the effectiveness of the security and privacy controls implemented within organizational systems. Training options include, for example, web-based and computer-based training; classroom-style training; and hands-on training. Organizations can also request training materials from developers to conduct in-house training or offer self-training to organizational personnel. Organizations determine the type of training necessary and may require different types of training for different security and privacy functions, controls, and mechanisms.

Related Controls: AT-2, AT-3, PE-3, SA-4, SA-5.

Control Enhancements: None.

References: None.

SA-17 DEVELOPER SECURITY ARCHITECTURE AND DESIGN

Control: Require the developer of the system, system component, or system service to produce a design specification and security architecture that:

a. Is consistent with and supportive of the organization's security architecture which is established within and is an integrated part of the organization's enterprise architecture;

b. Accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components; and

c. Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection.

Supplemental Guidance: This control is primarily directed at external developers, although it could also be used for internal (in-house) development. In contrast, PL-8 is primarily directed at internal developers to ensure that organizations develop a security architecture and that the architecture is integrated or tightly coupled to the enterprise architecture. This distinction is important when organizations outsource the development of systems, system components, or system services to external entities, and when there is a requirement to demonstrate consistency with the ~~organization's~~ enterprise architecture and security architecture of the organization. ISO/IEC 15408 provides additional information on security architecture and design including, for example, formal policy models, security-relevant components, formal and informal correspondence, conceptually simple design, and structuring for least privilege and testing.

Related Controls: PL-2, PL-8, PM-7, SA-3, SA-4, SA-8.

Control Enhancements:

(1) DEVELOPER SECURITY 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 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 policy when implemented.

Supplemental Guidance: Formal models describe specific behaviors or security policies using formal languages, thus enabling the correctness of those behaviors and policies to be formally proven. Not all components of systems can be modeled. Generally, formal specifications are scoped to the specific behaviors or policies of interest, for example, nondiscretionary access control policies. Organizations choose the formal modeling language and approach based on the nature of the behaviors and policies to be described and the available tools. Examples of formal modeling tools include Gypsy and Zed.

Related Controls: None.

(2) DEVELOPER SECURITY 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.

Supplemental Guidance: The security-relevant hardware, software, and firmware represent the portion of the system, component, or service that must be trusted to perform correctly to maintain required security properties.

Related Controls: SA-5.

(3) DEVELOPER SECURITY 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.

Supplemental Guidance: Correspondence is an important part of the assurance gained through modeling. It demonstrates that the implementation is an accurate transformation of the model, and that any additional code or implementation details that are present have no impact on the behaviors or policies being modeled. Formal methods can be used to show that the high-level security properties are satisfied by the formal system description, and that the formal system description is correctly implemented by a description of some lower level, for example a hardware description. Consistency between the formal top-level specification and the formal policy models is generally not amenable to being fully proven. Therefore, a combination of formal and informal methods may be needed to show such consistency. Consistency between the formal top-level specification and the actual implementation may require the use of an informal demonstration due to limitations in the applicability of formal methods to prove that the specification accurately reflects the implementation. Hardware, software, and firmware mechanisms strictly internal to security-relevant hardware, software, and firmware include, for example, mapping registers and direct memory input and output.

Related Controls: SA-5.

(4) DEVELOPER SECURITY ARCHITECTURE AND DESIGN | INFORMAL CORRESPONDENCE

Require the developer of the system, system component, or system service to:

(a) Produce, as an integral part of the development process, an informal descriptive top-level specification that specifies the interfaces to security-relevant hardware, software, and firmware in terms of exceptions, error messages, and effects;

(b) Show via [*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.

Supplemental Guidance: Correspondence is an important part of the assurance gained through modeling. It demonstrates that the implementation is an accurate transformation of the model, and that any additional code or implementation details present has no impact on the behaviors or policies being modeled. Consistency between the descriptive top-level specification (i.e., high-level/low-level design) and the formal policy model is generally not amenable to being fully proven. Therefore, a combination of formal and informal methods may be needed to show such consistency. Hardware, software, and firmware mechanisms strictly internal to security-relevant hardware, software, and firmware include, for example, mapping registers and direct memory input and output.

Related Controls: SA-5.

(5) DEVELOPER SECURITY 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.

Supplemental Guidance: None.

Related Controls: SC-3.

(6) DEVELOPER SECURITY ARCHITECTURE AND DESIGN | STRUCTURE FOR TESTING

Require the developer of the system, system component, or system service to structure security-relevant hardware, software, and firmware to facilitate testing.

Supplemental Guidance: None.

Related Controls: SA-5, SA-11.

(7) DEVELOPER SECURITY ARCHITECTURE AND DESIGN | STRUCTURE FOR LEAST PRIVILEGE

Require the developer of the system, system component, or system service to structure security-relevant hardware, software, and firmware to facilitate controlling access with least privilege.

Supplemental Guidance: None.

Related Controls: AC-5, AC-6.

References: ISO/IEC 15408; NIST Special Publication 800-160.

SA-18 TAMPER RESISTANCE AND DETECTION

Control: Implement a tamper protection program for the system, system component, or system service.

Supplemental Guidance: Anti-tamper technologies, tools, and techniques provide a level of protection for ~~critical~~ systems and system components~~, and information technology products~~ against many threats including ~~modification,~~ reverse engineering, modification, and substitution. Strong identification combined with tamper resistance and/or tamper detection is essential to protecting systems and components~~, and products~~ during distribution and when in use.

Related Controls: PE-3, SA-12, SI-7.

Control Enhancements:

(1) TAMPER RESISTANCE AND DETECTION | MULTIPLE PHASES OF ~~*SDLC*~~SYSTEM DEVELOPMENT LIFE CYCLE

Employ anti-tamper technologies, tools, and techniques during multiple phases in the system development life cycle including design, development, integration, operations, and maintenance.

Supplemental Guidance: Organizations use a combination of hardware and software techniques for tamper resistance and detection. Organizations employ obfuscation and self-checking, for example, to make reverse engineering and modifications more difficult, time-consuming, and expensive for adversaries. The customization of systems and system components can make substitutions easier to detect and therefore limit damage.

Related Controls: SA-3.

(2) TAMPER RESISTANCE AND DETECTION | INSPECTION OF ~~*INFORMATION*~~ SYSTEMS OR COMPONENTS

Inspect [*Assignment: organization-defined systems or system components*] [*Selection (one or more): at random;* at [*Assignment: organization-defined frequency*], *upon* [*Assignment: organization-defined indications of need for inspection*]] to detect tampering.

Supplemental Guidance: This control enhancement addresses physical and logical tampering and is typically applied to mobile devices, notebook computers, or other system components taken out of organization-controlled areas. Indications of a need for inspection include, for example, when individuals return from travel to high-risk locations.

Related Controls: SI-4.

References: None.

SA-19 COMPONENT AUTHENTICITY

Control:

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*]].

Supplemental Guidance: Sources of counterfeit components include, for example, manufacturers, developers, vendors, and contractors. Anti-counterfeiting policy and procedures support tamper resistance and provide a level of protection against the introduction of malicious code. External reporting organizations include, for example, US-CERT.

Related Controls: PE-3, SA-12, SI-7.

Control Enhancements:

(1) COMPONENT AUTHENTICITY | ANTI-COUNTERFEIT TRAINING

Train [*Assignment: organization-defined personnel or roles*] to detect counterfeit system components (including hardware, software, and firmware).

Supplemental Guidance: None.

Related Controls: AT-3.

(2) COMPONENT AUTHENTICITY | CONFIGURATION CONTROL FOR COMPONENT SERVICE AND REPAIR

Maintain configuration control over [*Assignment: organization-defined system components*] awaiting service or repair and serviced or repaired components awaiting return to service.

Supplemental Guidance: None.

Related Controls: CM-3.

(3) COMPONENT AUTHENTICITY | COMPONENT DISPOSAL

Dispose of system components using [*Assignment: organization-defined techniques and methods*].

Supplemental Guidance: Proper disposal of system components helps to prevent such components from entering the gray market.

Related Controls: MP-6.

(4) COMPONENT AUTHENTICITY | ANTI-COUNTERFEIT SCANNING

Scan for counterfeit system components [*Assignment: organization-defined frequency*].

Supplemental Guidance: None.

Related Controls: RA-5.

References: None.

SA-20 CUSTOMIZED DEVELOPMENT OF CRITICAL COMPONENTS

Control: Re-implement or custom develops [*Assignment: organization-defined critical system components*].

Supplemental Guidance: Organizations determine that certain system components likely cannot be trusted due to specific threats to and vulnerabilities in those components, and for which there are no viable security controls to adequately mitigate the resulting risk. Re-implementation or custom development of such components helps to satisfy requirements for higher assurance. This is accomplished by initiating changes to system components (including hardware, software, and firmware) such that the standard attacks by adversaries are less likely to succeed. In situations where no alternative sourcing is available and organizations choose not to re-implement or custom develop critical system components, additional safeguards can be employed. These include, for example, enhanced auditing; restrictions on source code and system utility access; and protection from deletion of system and application files.

Related Controls: CP-2, RA-9, SA-8.

Control Enhancements: None.

References: None.

SA-21 DEVELOPER SCREENING

Control: Require that the developer of [*Assignment: organization-defined system, system component, or system service*]:

a. Have appropriate access authorizations as determined by assigned [*Assignment: organization-defined official government duties*];

b. Satisfy [*Assignment: organization-defined additional personnel screening criteria*]; and

c. Provide information that the access authorizations and screening criteria specified in a. and b. are satisfied.

Supplemental Guidance: This control is directed at external developers. Because the system, system component, or system service may be employed in critical activities essential to the national or economic security interests of the United States, organizations have a strong interest in ensuring that the developer is trustworthy. The degree of trust required of the developer may need to be consistent with that of the individuals accessing the system/component/service once deployed. Examples of authorization and personnel screening criteria include clearances, background checks, citizenship, and nationality. Trustworthiness of developers may also include a review and analysis of company ownership and any relationships the company has with entities potentially affecting the quality and reliability of the systems, components, or services being developed.

Satisfying required access authorizations and personnel screening criteria includes, for example, providing a ~~listing~~list of all ~~the~~ individuals who are authorized to perform development activities on the selected system, system component, or system service so that organizations can validate that the developer has satisfied the authorization and screening requirements.

Related Controls: PS-2, PS-3, PS-6, PS-7, SA-4.

Control Enhancements:

(1) *DEVELOPER SCREENING | VALIDATION OF SCREENING*

~~**(2) The organization requires the developer of the information system, system component, or information system service take [*Assignment: organization-defined actions*] to ensure that the required access authorizations and screening criteria are satisfied.**~~
[Withdrawn: Incorporated into SA-21].

References: None.

SA-22 UNSUPPORTED SYSTEM COMPONENTS

Control: Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer.

~~**(1) Provides justification and documents approval for the continued use of unsupported system components required to satisfy mission/business needs.**~~

Supplemental Guidance: Support for system components includes, for example, software patches, firmware updates, replacement parts, and maintenance contracts. Unsupported components, for example, when vendors no longer provide critical software patches or product updates, provide ~~a substantial~~an opportunity for adversaries to exploit ~~new~~ weaknesses ~~discovered~~ in the ~~currently~~ installed components. Exceptions to replacing unsupported system components may include, for example, systems that provide critical mission or business capability where newer technologies are not available or where the systems are so isolated that installing replacement components is not an option.

Related Controls: PL-2, SA-3.

Control Enhancements:

(1) UNSUPPORTED SYSTEM COMPONENTS | ALTERNATIVE SOURCES FOR CONTINUED SUPPORT

Provide [*Selection (one or more): in-house support;* [*Assignment: organization-defined support from external providers*]] for unsupported system components.

Supplemental Guidance: This control enhancement addresses 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 operations. Organizations can establish in-house support, for example, by developing customized patches for critical software components or alternatively, obtain the services of external providers who through contractual relationships, provide ongoing support for the designated unsupported components. Such contractual relationships can include, for example, Open Source Software value-added vendors.

Related Controls: None.

References: None.

DEVELOPMENT OF SYSTEMS, COMPONENTS, AND SERVICES

With a renewed nation-wide emphasis on the use of trustworthy systems and supply chain security, it is essential that organizations can express their security and privacy requirements with clarity and specificity to engage industry and obtain the systems, components, and services necessary for mission/business success. Accordingly, this publication provides a comprehensive set of controls in the System and Services Acquisition (SA) family that address requirements for the development of systems, components, and system services. To that end, many of the controls in the SA family are directed at developers of those systems, components, and services. It is important for organizations to recognize that the scope of the controls in that family includes system, component, and service development and the developers associated with such development whether the development is conducted either internally or externally by industry partners (i.e., manufacturers, vendors, integrators) through the contracting and acquisition processes. The affected controls in the control catalog include SA-8, SA-10, SA-11, SA-15, SA-16, SA-17, SA-20, and SA-21.

3.19 SYSTEM AND COMMUNICATIONS PROTECTION

Quick link to System and Communications Protection summary table

SC-1 SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES

Control:

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

1. A 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 senior management official*] to manage the system and communications protection policy and procedures;

~~b.~~c. Review and update the current system and communications protection:

1. Policy [*Assignment: organization-defined frequency*]; and

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

d. Ensure that the system and communications protection procedures implement the system and communications protection policy and controls; and

e. Develop, document, and implement remediation actions for violations of the system and communications protection policy.

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of ~~selected security~~ the controls and control enhancements in the SC family. The risk management strategy is an important factor in establishing policy and procedures ~~reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards,~~. Comprehensive policy and ~~guidance.~~procedures help provide security and privacy assurance. Security and privacy program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general ~~information~~ security and privacy policy ~~for organizations~~ or ~~conversely,~~ can be represented by multiple policies reflecting the complex nature of ~~certain~~ organizations. The procedures can be established for ~~the~~ security ~~program in general~~and privacy programs and for ~~particular information~~ systems, if needed. ~~The~~Procedures describe how policies or controls are implemented and can be directed at the personnel or role that is the object of the procedure. Procedures can be documented in system security and plans or in one or more separate documents. It is important to recognize that restating controls does not constitute an organizational ~~risk management strategy is a key factor in establishing~~ policy ~~and procedures.~~ or procedure.

Related Controls: PM-9, PS-8, SI-12.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

SC-2 APPLICATION PARTITIONING

Control: Separate user functionality, including user interface services, from system management functionality.

Supplemental Guidance: System management functionality includes, for example, functions that are necessary to administer databases, network components, workstations, or servers. These functions typically require privileged user access. The separation of user functions from system management functions is either physical or logical. Organizations implement separation of system management functions from user functions, for example, by using different computers, instances of operating systems, central processing units, or network addresses; by employing virtualization techniques; or some combination of these or other methods. This type of separation includes, for example, web administrative interfaces that use separate authentication methods for users of any other system resources. Separation of system and user functions may include isolating administrative interfaces on different domains and with additional access controls.

Related Controls: AC-6, SA-4, SA-8, SC-3, SC-7, SC-22, SC-32, SC-39.

Control Enhancements:

(1) APPLICATION PARTITIONING | INTERFACES FOR NON-PRIVILEGED USERS

Prevent the presentation of system management ~~-related~~ functionality at an interface for non-privileged users.

Supplemental Guidance: This control enhancement ensures that system administration options including administrator privileges, are not available to general users ~~(including prohibiting.~~ This type of restricted access also prohibits the use of the grey-out option commonly used to eliminate accessibility to such information~~). Such restrictions include, for example, not presenting~~. One potential solution is to withhold administration options until users establish sessions with administrator privileges.

Related Controls: AC-3.

References: None.

SC-3 SECURITY FUNCTION ISOLATION

Control: Isolate security functions from nonsecurity functions.

Supplemental Guidance: The system isolates security functions from nonsecurity functions by means of an isolation boundary implemented via partitions and domains. Such isolation controls access to and protects the integrity of the hardware, software, and firmware that perform those security functions. Systems implement code separation ~~(i.e., separation of security functions from nonsecurity functions)~~ in many ways, for example, through the provision of security kernels via processor rings or processor modes. For non-kernel code, security function isolation is often achieved through file system protections that protect the code on disk and address space protections that protect executing code. Systems can restrict access to security functions using access control mechanisms and by implementing least privilege capabilities. While the ideal is for all code within the defined security function isolation boundary to only contain security-relevant code, it is sometimes necessary to include nonsecurity functions within the isolation boundary as an exception.

Related Controls: 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.

Control Enhancements:

(1) SECURITY FUNCTION ISOLATION | HARDWARE SEPARATION

~~utilizes underlying~~Use hardware separation mechanisms to implement security function isolation.

Supplemental Guidance: Hardware separation mechanisms include, for example, hardware ring architectures that are commonly implemented within microprocessors, and hardware-enforced address segmentation used to support logically distinct storage objects with separate attributes (i.e., readable, writeable).

Related Controls: None.

(2) SECURITY FUNCTION ISOLATION | ACCESS AND FLOW CONTROL FUNCTIONS

~~The information system isolates~~Isolate **security functions enforcing access and information flow control from nonsecurity functions and from other security functions.**

Supplemental Guidance: 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, for example, auditing, intrusion detection, and anti-virus functions.

Related Controls: None.

(3) SECURITY FUNCTION ISOLATION | MINIMIZE NONSECURITY FUNCTIONALITY

Minimize the number of nonsecurity functions included within the isolation boundary containing security functions.

Supplemental Guidance: In those instances where it is not feasible to achieve strict isolation of nonsecurity functions from security functions, it is necessary to take actions to minimize the nonsecurity-relevant functions within the security function boundary. Nonsecurity functions contained within the isolation boundary are considered security-relevant because errors or the maliciousness in such software, ~~by virtue of being within the boundary,~~ can directly impact the security functions of systems. The fundamental design objective is that the specific portions of systems providing 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 nonsecurity functions within the isolation boundaries, the amount of code that must be trusted to enforce security policies is significantly reduced, thus contributing to understandability.

Related Controls: None.

(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.

Supplemental Guidance: The reduction in inter-module interactions helps to constrain security functions and to 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 different functions within a module. Best practices in software engineering rely on layering, minimization, and modular decomposition to reduce and manage complexity. This produces software modules that are highly cohesive and loosely coupled.

Related Controls: None.

(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.

Supplemental Guidance: 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) further enables the isolation of security functions and management of complexity.

Related Controls: None.

References: None.

SC-4 INFORMATION IN SHARED SYSTEM RESOURCES

Control: Prevent unauthorized and unintended information transfer via shared system resources.

Supplemental Guidance: This control prevents information~~, including encrypted representations of information,~~ produced by the actions of prior users or roles (or the actions of processes acting on behalf of prior users or roles) from being available to current users or roles (or current processes acting on behalf of current users or roles) that obtain access to shared system resources ~~(e.g., registers, main memory, hard disks)~~ after those resources have been released back to the system.

This control also applies to encrypted representations of information ~~systems~~. The control of information in shared system resources is referred to as object reuse and residual information protection. This control does not address information remanence which refers to the residual representation of data that has been nominally ~~erased or removed; (ii)~~deleted; covert channels (including storage and timing channels) where shared system resources are manipulated to violate information flow restrictions; or components within systems for which there are only single users or roles.

Related Controls: AC-3, AC-4.

Control Enhancements:

(1) INFORMATION IN SHARED SYSTEM RESOURCES | SECURITY LEVELS

[Withdrawn: Incorporated into 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.

Supplemental Guidance: This control enhancement applies when there are explicit changes in information processing levels during system operations. This situation can occur, for example, during multilevel or periods processing with information at different classification levels or security categories. Organization-defined procedures may include, for example, approved sanitization processes for electronically stored information.

Related Controls: None.

References: None.

SC-5 DENIAL OF SERVICE PROTECTION

Control: Protect against or limit the effects of the following types of denial of service ~~attacks~~events: [*Assignment: organization-defined types of denial of service ~~attacks~~events or references to sources for such information*] by employing [*Assignment: organization-defined security safeguards*].

Supplemental Guidance: Denial of service may occur because of an attack by an adversary or a lack of internal planning to support organizational needs with respect to capacity and bandwidth. There are a variety of technologies ~~exist~~available to limit or ~~in some cases,~~ eliminate the effects of denial of service ~~attacks~~events. For example, boundary protection devices can filter certain types of packets to protect system components on internal ~~organizational~~ networks from being directly affected by denial of service attacks. Employing increased network capacity and bandwidth combined with service redundancy also reduces the susceptibility to denial of service ~~attacks.~~ events.

Related Controls: CP-2, IR-4, SC-6, SC-7, SC-40.

Control Enhancements:

(1) DENIAL OF SERVICE PROTECTION | RESTRICT INTERNAL USERS

Restrict the ability of individuals to launch [*Assignment: organization-defined denial of service attacks*] against other systems.

Supplemental Guidance: Restricting the ability of individuals to launch denial of service attacks requires that the mechanisms commonly used for such attacks are unavailable. Individuals of concern can include, for example, hostile insiders or external adversaries that have breached or compromised the system and are subsequently using the system ~~as a platform~~ to launch ~~cyber~~ attacks on ~~third parties~~other individuals or organizations. Organizations can restrict the ability of individuals to connect and transmit arbitrary information on the transport medium (i.e., ~~network,~~wired or wireless ~~spectrum~~networks). 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 on boundary devices prohibiting egress to potential target systems.

Related Controls: None.

(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.

Supplemental Guidance: Managing capacity ensures that sufficient capacity is available to counter flooding attacks. Managing capacity may include, for example, establishing selected usage priorities, quotas, or partitioning.

Related Controls: None.

(3) DENIAL OF SERVICE PROTECTION | DETECTION AND MONITORING

(a) Employ [*Assignment: organization-defined monitoring tools*] to detect indicators of denial of service attacks against the system; and

(b) Monitor [*Assignment: organization-defined system resources*] to determine if sufficient resources exist to prevent effective denial of service attacks.

Supplemental Guidance: Organizations consider utilization and capacity of system resources when managing risk from denial of service due to malicious attacks. Denial of service attacks can originate from external or internal sources. System resources sensitive to denial of service include, for example, physical disk storage, memory, and CPU cycles. Examples of common safeguards used to prevent denial of service attacks related to storage utilization and capacity include, instituting disk quotas; configuring systems to automatically alert administrators when specific storage capacity thresholds are reached; using file compression technologies to maximize available storage space; and imposing separate partitions for system and user data.

Related Controls: CA-7, SI-4.

References: None.

SC-6 RESOURCE AVAILABILITY

Control: Protect the availability of resources by allocating [*Assignment: organization-defined resources*] by [*Selection (one or more); priority; quota;* [*Assignment: organization-defined security safeguards*]].

Supplemental Guidance: Priority protection prevents lower-priority processes from delaying or interfering with the system servicing higher-priority processes. Quotas prevent users or processes from obtaining more than predetermined amounts of resources. This control does not apply to system components for which there are only single users or roles.

Related Controls: SC-5.

Control Enhancements: None.

References: None.

SC-7 BOUNDARY PROTECTION

Control:

a. Monitor and control communications at the external boundary of the system and at key internal boundaries 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.

Supplemental Guidance: Managed interfaces include, for example, gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within a security architecture ~~(e.g., routers protecting firewalls or application~~

~~gateways residing on protected subnetworks).~~. Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones or DMZs. Restricting or prohibiting interfaces within organizational systems includes, for example, restricting external web traffic to designated web servers within managed interfaces and prohibiting external traffic that appears to be spoofing internal addresses. ~~Organizations consider the shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services.~~ Commercial telecommunications services are ~~commonly based on~~typically provided by network components and consolidated management systems shared by ~~all attached commercial~~ customers. These services may also include third party-provided access lines and other service elements. Such services may represent sources of increased risk despite contract security provisions.

Related Controls: 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, PM-12, SC-5, SC-19, SC-32, SC-43.

Control Enhancements:

(1) BOUNDARY PROTECTION | PHYSICALLY SEPARATED SUBNETWORKS

[Withdrawn: Incorporated into SC-7].

(2) BOUNDARY PROTECTION | PUBLIC ACCESS

[Withdrawn: Incorporated into SC-7].

(3) BOUNDARY PROTECTION | ACCESS POINTS

Limit the number of external network connections to the system.

Supplemental Guidance: Limiting the number of external network connections facilitates more comprehensive monitoring of inbound and outbound communications traffic. The Trusted Internet Connection initiative is an example of limiting the number of external network connections.

Related Controls: None.

(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/business need and duration of that need; and

(e) Review exceptions to the traffic flow policy [*Assignment: organization-defined frequency*] and removes exceptions that are no longer supported by an explicit mission/business need.

Supplemental Guidance: None.

Related Controls: AC-3, SC-8.

(5) BOUNDARY PROTECTION | DENY BY DEFAULT — ALLOW BY EXCEPTION

Deny network communications traffic by default and allow network communications traffic by exception ~~(i.e., deny all, permit by exception).~~at managed interfaces.

Supplemental Guidance: This control enhancement applies to ~~both~~ inbound and outbound network communications traffic. A deny-all, permit-by-exception network communications traffic policy ensures that only those system connections which are essential and approved are allowed. This requirement differs from CA-3(5) in that it applies to any type of network communications while CA-3(5) is applied to a system that is interconnected with another system.

(6) BOUNDARY PROTECTION | RESPONSE TO RECOGNIZED FAILURES

[Withdrawn: Incorporated into SC-7(18)].

(7) BOUNDARY PROTECTION | PREVENT SPLIT TUNNELING FOR REMOTE DEVICES

~~The information system, in conjunction with a remote device, prevents the~~Prevent a remote device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks.

Supplemental Guidance: This control enhancement is implemented in remote devices ~~(e.g.,~~including, for example, notebook computers, through configuration settings to disable split tunneling in those devices, and by preventing those configuration settings from being readily configurable by users. This control enhancement is implemented within the system 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. Split tunneling might be desirable by remote users to communicate with local system resources such as printers or file servers. However, split tunneling can allow unauthorized external connections, making the system more vulnerable to attack and to exfiltration of organizational information. The use of VPNs for remote connections, when adequately provisioned with the appropriate security controls, may provide the organization with sufficient assurance that it can effectively treat such connections as non-remote connections with respect to the objectives of confidentiality and integrity. VPNs provide a means for allowing non-remote communications paths from remote devices. The use of an adequately provisioned VPN does not eliminate the need for preventing split tunneling.

Related Controls: None.

(8) BOUNDARY PROTECTION | ROUTE TRAFFIC TO AUTHENTICATED PROXY SERVERS

Route [*Assignment: organization-defined internal communications traffic*] to [*Assignment: organization-defined external networks*] through authenticated proxy servers at managed interfaces.

Supplemental Guidance: External networks are networks outside of organizational control. A proxy server is a server (i.e., system or application) that acts as an intermediary for clients requesting system resources ~~(e.g.,~~from non-organizational or other organizational servers. These system resources can include, for example, files, connections, web pages, or services~~)~~ ~~from other organizational servers.~~. Client requests established through an initial connection to the proxy server are evaluated to manage complexity and to provide additional protection by limiting direct connectivity. Web content filtering devices are one of the most common proxy servers providing access to the Internet. Proxy servers can support logging of individual Transmission Control Protocol sessions and blocking specific Uniform Resource Locators, Internet Protocol addresses, and domain names. Web proxies can be configured with organization-defined lists of authorized and unauthorized websites.

Related Controls: AC-3.

(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.

Supplemental Guidance: Detecting outgoing communications traffic from internal actions that may pose threats to external systems is known as extrusion detection. Extrusion detection is carried out at system boundaries as part of managed interfaces. This capability includes the analysis of incoming and outgoing communications traffic while searching for indications of internal threats to the security of external systems. Such threats include, for example, traffic indicative of denial of service attacks and traffic containing malicious code.

Related Controls: AU-2, AU-6, SC-5, SC-38, SC-44, SI-3, SI-4.

(10) BOUNDARY PROTECTION | PREVENT ~~*UNAUTHORIZED*~~ EXFILTRATION

(a) Prevent the ~~unauthorized~~ exfiltration of information ~~across managed interfaces.~~; and

(b) Conduct exfiltration tests [*Assignment: organization-defined frequency*].

Supplemental Guidance: ~~Safeguards implemented by organizations~~This control enhancement applies to ~~prevent unauthorized~~intentional and unintentional exfiltration of information. Safeguards to prevent exfiltration of information from systems may be implemented at internal endpoints, external boundaries, and across managed interfaces and include, for example, strict adherence to protocol formats; monitoring for beaconing activity from systems; monitoring for steganography; disconnecting external network interfaces except when explicitly needed; disassembling and reassembling packet headers; employing traffic profile analysis to detect deviations from the volume and types of traffic expected within

organizations or call backs to command and control centers; and implementing data loss and data leakage prevention tools. Devices that enforce strict adherence to protocol formats include, for example, deep packet inspection firewalls and XML gateways. These devices verify adherence to protocol formats and specifications at the application layer and identify vulnerabilities that cannot be detected by devices operating at the network or transport layers. This control enhancement is analogous with data loss/data leakage prevention and is closely associated with cross-domain solutions and system guards enforcing information flow requirements.

Related Controls: SI-3.

(11) BOUNDARY PROTECTION | RESTRICT INCOMING COMMUNICATIONS TRAFFIC

Only allow incoming communications from [*Assignment: organization-defined authorized sources*] to be routed to [*Assignment: organization-defined authorized destinations*].

Supplemental Guidance: This control enhancement provides determinations that source and destination address pairs represent authorized/allowed communications. Such determinations can be based on several factors including, for example, the presence of ~~source/destination~~such address pairs in the lists of authorized/allowed communications; the absence of such address pairs in lists of unauthorized/disallowed pairs; or meeting more general rules for authorized/allowed source and destination pairs.

Related Controls: AC-3.

(12) BOUNDARY PROTECTION | HOST-BASED PROTECTION

Implement [*Assignment: organization-defined host-based boundary protection mechanisms*] at [*Assignment: organization-defined system components*].

Supplemental Guidance: Host-based boundary protection mechanisms include, for example, host-based firewalls. Examples of system components employing host-based boundary protection mechanisms include servers, workstations, notebook computers, and mobile devices.

Related Controls: None.

(13) BOUNDARY PROTECTION | ISOLATION OF SECURITY TOOLS, MECHANISMS, AND SUPPORT COMPONENTS

Isolate [*Assignment: organization-defined information security tools, mechanisms, and support components*] from other internal system components by implementing physically separate subnetworks with managed interfaces to other components of the system.

Supplemental Guidance: Physically separate subnetworks with managed interfaces are useful, for example, in isolating computer network defenses from critical operational processing networks to prevent adversaries from discovering the analysis and forensics techniques of organizations.

Related Controls: SC-2, SC-3.

(14) BOUNDARY PROTECTION | PROTECTS AGAINST UNAUTHORIZED PHYSICAL CONNECTIONS

Protect against unauthorized physical connections at [*Assignment: organization-defined managed interfaces*].

Supplemental Guidance: Systems operating at different security categories or classification levels may share common physical and environmental controls, since the systems may share space within ~~organizational~~the same facilities. In practice, it is possible that these separate systems may share common equipment rooms, wiring closets, and cable distribution paths. Protection against unauthorized physical connections can be achieved, for example, by employing clearly identified and physically separated cable trays, connection frames, and patch panels for each side of managed interfaces with physical access controls enforcing limited authorized access to these items.

Related Controls: PE-4, PE-19.

(15) BOUNDARY PROTECTION | ROUTE PRIVILEGED NETWORK ACCESSES

Route all networked, privileged accesses through a dedicated, managed interface for purposes of access control and auditing.

Supplemental Guidance: None.

Related Controls: AC-2, AC-3, AU-2, SI-4.

(16) BOUNDARY PROTECTION | PREVENT DISCOVERY OF COMPONENTS AND DEVICES

Prevent the discovery of specific system components ~~composing~~that represent a managed interface.

Supplemental Guidance: This control enhancement protects network addresses of system components that are part of managed interfaces from discovery through common tools and techniques used to identify devices on networks. Network addresses are not available for discovery ~~(e.g., network address not published or entered in domain name systems),~~ requiring prior knowledge for access. This can be accomplished by not publishing network addresses or entering the addresses in domain name systems. Another obfuscation technique is to periodically change network addresses.

Related Controls: None.

(17) BOUNDARY PROTECTION | AUTOMATED ENFORCEMENT OF PROTOCOL FORMATS

Enforce adherence to protocol formats.

Supplemental Guidance: Examples of system components that enforce protocol formats include deep packet inspection firewalls and XML gateways. Such components verify adherence to protocol formats and specifications at the application layer and identify vulnerabilities that cannot be detected by devices operating at the network or transport layers.

Related Controls: SC-4.

(18) BOUNDARY PROTECTION | FAIL SECURE

~~The information system fails securely~~Prevent systems from entering unsecure states in the event of an operational failure of a boundary protection device.

Supplemental Guidance: Fail secure is a condition achieved by employing system mechanisms to ensure that in the event of operational failures of boundary protection devices at managed interfaces ~~(e.g., routers, firewalls, guards~~, systems do not enter into unsecure states where intended security properties no longer hold. Examples of managed interfaces include routers, firewalls, and application gateways residing on protected subnetworks commonly referred to as demilitarized zones~~), information systems do not enter into unsecure states where intended security properties no longer hold.~~. Failures of boundary protection devices cannot lead to, or cause information external to the devices to enter the devices, nor can failures permit unauthorized information releases.

Related Controls: CP-2, CP-12, SC-24.

(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.

Supplemental Guidance: Communication clients independently configured by end users and external service providers include, for example, instant messaging clients. Traffic blocking does not apply to communication clients that are configured by organizations to perform authorized functions.

Related Controls: None.

(20) BOUNDARY PROTECTION | DYNAMIC ISOLATION AND SEGREGATION

Provide the capability to dynamically isolate or segregate [*Assignment: organization-defined system components*] from other system components.

Supplemental Guidance: The capability to dynamically isolate or segregate certain internal components of organizational systems is useful when it is necessary to partition or separate certain system components of ~~dubious~~questionable origin from those components possessing greater trustworthiness. Component isolation reduces the attack surface of organizational systems. Isolating selected system components can also limit the damage from successful ~~cyber~~ attacks when ~~those~~such attacks occur.

Related Controls: None.

(21) BOUNDARY PROTECTION | ISOLATION OF SYSTEM COMPONENTS

Employ boundary protection mechanisms to separate [*Assignment: organization-defined system components*] supporting [*Assignment: organization-defined missions and/or business functions*].

Supplemental Guidance: Organizations can isolate system components performing different missions or business functions. Such isolation limits unauthorized information flows among system components and provides the opportunity to deploy greater levels of protection for selected system components. Separating system components with boundary protection mechanisms provides the capability for increased protection of individual components and to more effectively control information flows between those components. This type of enhanced protection limits the potential harm from ~~cyber~~hostile attacks and errors. The degree of separation provided varies depending upon the mechanisms chosen. Boundary protection mechanisms include, for example, routers, gateways, and firewalls separating system components into physically separate networks or subnetworks; cross-domain devices separating subnetworks; virtualization techniques; and encrypting information flows among system components using distinct encryption keys.

Related Controls: CA-9, SC-3.

(22) BOUNDARY PROTECTION | SEPARATE SUBNETS FOR CONNECTING TO DIFFERENT SECURITY DOMAINS

Implement separate network addresses ~~(i.e., different subnets)~~ to connect to systems in different security domains.

Supplemental Guidance: The decomposition of systems into subnetworks (subnets) helps to provide the appropriate level of protection for network connections to different security domains containing information with different security categories or classification levels.

Related Controls: None.

(23) BOUNDARY PROTECTION | DISABLE SENDER FEEDBACK ON PROTOCOL VALIDATION FAILURE

Disable feedback to senders on protocol format validation failure.

Supplemental Guidance: Disabling feedback to senders when there is a failure in protocol validation format prevents adversaries from obtaining information which would otherwise be unavailable.

Related Controls: None.

(24) BOUNDARY PROTECTION | PERSONALLY IDENTIFIABLE INFORMATION

For systems that process, store, or transmit personally identifiable information:

(a) Apply [*Assignment: organization-defined processing rules*] to data elements of personally identifiable information;

(b) Monitor for permitted processing at the external boundary of 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.

Supplemental Guidance: Managing the transmission of personally identifiable information and how such information is used is an important aspect of safeguarding an individual's privacy. Processing rules that determine how or when personally identifiable information may be used or transmitted ensures that such information is used or transmitted only in accordance with established privacy requirements.

Related Controls: SI-15.

References: FIPS Publication 199; NIST Special Publications 800-41, 800-77.

SC-8 TRANSMISSION CONFIDENTIALITY AND INTEGRITY

Control: Protect the [*Selection (one or more): confidentiality; integrity*] of transmitted information.

Supplemental Guidance: This control applies to internal and external networks and ~~all types of information~~any system components ~~from which information~~that can transmit information including, for example, servers, notebook computers, desktop computers, mobile devices, printers, copiers, scanners, facsimile machines~~).~~, and radios. Unprotected communication paths ~~outside the~~

~~physical protection of a controlled boundary~~ are exposed to the possibility of interception and modification. Protecting the confidentiality and integrity of ~~organizational~~ information can be accomplished by physical means ~~(e.g.,~~or by logical means. Physical protection can be achieved by employing protected distribution systems~~) or by logical means (e.g.,~~. Logical protection can be achieved by employing encryption techniques~~).~~. Organizations relying on commercial providers offering transmission services as commodity services rather than as fully dedicated services ~~(i.e., services which can be highly specialized to individual customer needs).~~, may find it difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality and integrity. In such situations, organizations determine what types of confidentiality/integrity services are available in standard, commercial telecommunication service packages. If it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, organizations can implement appropriate compensating security controls or explicitly accept the additional risk.

Related Controls: AC-17, AC-18, AU-10, IA-3, IA-8, IA-9, MA-4, PE-4, SA-4, SC-7, SC-16, SC-20, SC-23, SC-28.

Control Enhancements:

(1) TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC ~~*OR ALTERNATE PHYSICAL*~~ PROTECTION

~~**The information system implements**~~**Implement cryptographic mechanisms to [*Selection (one or more): prevent unauthorized disclosure of information; detect changes to information*] during transmission** ~~**unless otherwise protected by [*Assignment: organization-defined alternative physical safeguards*].**~~

Supplemental Guidance: Encrypting information for transmission protects information from unauthorized disclosure and modification. Cryptographic mechanisms implemented to protect information integrity include, for example, cryptographic hash functions which have common application in digital signatures, checksums, and message authentication codes. ~~Alternative physical security safeguards include, for example, protected distribution systems. Related control: SC-13.~~

Related Controls: SC-13.

(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.

Supplemental Guidance: Information can be either unintentionally or maliciously disclosed or modified during preparation for transmission or during reception including, for example, during aggregation, at protocol transformation points, and during packing and unpacking. These unauthorized disclosures or modifications compromise the confidentiality or integrity of the information.

Related Controls: AU-10.

(3) TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC PROTECTION FOR MESSAGE EXTERNALS

Implement cryptographic mechanisms to protect message externals unless otherwise protected by [*Assignment: organization-defined alternative physical safeguards*].

Supplemental Guidance: This control enhancement addresses protection against unauthorized disclosure of information. Message externals include, for example, message headers and routing information. This control enhancement prevents the exploitation of message externals and applies to internal and external networks or links that may be visible to individuals who are not authorized users. Header and routing information is sometimes transmitted in the clear (i.e., unencrypted) because the information is not properly identified by organizations as having significant value or because encrypting the information can result in lower network performance or higher costs. Alternative physical safeguards include, for example, protected distribution systems.

Related Controls: SC-12, SC-13.

(4) TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CONCEAL OR RANDOMIZE COMMUNICATIONS

Implement cryptographic mechanisms to conceal or randomize communication patterns unless otherwise protected by [*Assignment: organization-defined alternative physical safeguards*].

Supplemental Guidance: This control enhancement addresses protection against unauthorized disclosure of information. Communication patterns include, for example, frequency, periods, amount, and predictability. Changes to communications patterns can reveal information having intelligence value especially when combined with other available information related to the missions and business functions supported by organizational systems. This control enhancement prevents the derivation of intelligence based on communications patterns and applies to internal and external networks or links that may be visible to individuals who are not authorized users. Encrypting the links and transmitting in continuous, fixed or random patterns prevents the derivation of intelligence from the system communications patterns. Alternative physical safeguards include, for example, protected distribution systems.

Related Controls: SC-12, SC-13.

References: FIPS Publications 140-2, 197; NIST Special Publications 800-52, 800-77, 800-81, 800-113, 800-177; NIST Interagency Report 8023.

SC-9 TRANSMISSION CONFIDENTIALITY

[Withdrawn: Incorporated into SC-8].

SC-10 NETWORK DISCONNECT

Control: Terminate the network connection associated with a communications session at the end of the session or after [*Assignment: organization-defined time-period*] of inactivity.

Supplemental Guidance: This control applies to internal and external networks. Terminating network connections associated with specific communications sessions include, for example, de-allocating associated TCP/IP address or port pairs at the operating system level and de-allocating networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. Periods of inactivity may be established by organizations and include, for example, time-periods by type of network access or for specific network accesses.

Related Controls: AC-17, SC-23.

Control Enhancements: None.

References: None.

SC-11 TRUSTED PATH

Control:

a. Provide a [*Selection: physically; logically*] isolated trusted communications path for communications between the user and the trusted components of the system; and

~~a.~~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 ~~to include at a minimum, information system authentication and re-authentication~~*]~~.~~].

Supplemental Guidance: Trusted paths are mechanisms by which users (through input devices) can communicate directly with security functions of systems with the requisite assurance to support security policies. These mechanisms can be activated only by users or the security functions of organizational systems. User responses via trusted paths are protected from modifications by or disclosure to untrusted applications. Organizations employ trusted paths for trustworthy, high-assurance connections between security functions of systems and users including, for example, during system logons. The original implementations of trusted path used an out-of-band signal to initiate the path, for example using the <BREAK> key, which does not transmit characters that can be spoofed. In later implementations, a key combination that could not be hijacked was used, for example, the <CTRL> + <ALT> + <DEL> keys. Note, however, that any such key combinations are

platform-specific and may not provide a trusted path implementation in every case. Enforcement of trusted communications paths is typically provided by a specific implementation that meets the reference monitor concept.

Related Controls: AC-16, AC-25, SC-12, SC-23.

Control Enhancements:

(1) TRUSTED PATH | LOGICAL ISOLATION

(a) Provide a trusted communications path that is ~~logically isolated and~~irrefutably distinguishable from other communications paths; and

(b) Initiate the trusted communications path for communications between the following security functions of the system and the user [*Assignment: organization-defined security functions*].

Supplemental Guidance: This enhancement 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.

Related Controls: None.

References: None.

SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

Control: Establish and manage cryptographic keys for required cryptography employed within the system in accordance with [*Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction*].

Supplemental Guidance: Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. Organizations define their key management requirements in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines, specifying appropriate options, levels, and parameters. Organizations manage trust stores to ensure that only approved trust anchors are in such trust stores. This includes certificates with visibility external to organizational systems and certificates related to the internal operations of systems.

Related Controls: AC-17, AU-9, AU-10, CM-3, IA-3, IA-7, SA-4, SA-9, SC-8, SC-11, SC-13, SC-17, SC-20, SC-37, SC-40, SI-3, SI-7.

Control Enhancements:

(1) CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | AVAILABILITY

Maintain availability of information in the event of the loss of cryptographic keys by users.

Supplemental Guidance: Escrowing of encryption keys is a common practice for ensuring availability in the event of loss of keys. A forgotten passphrase is an example of losing a cryptographic key.

Related Controls: None.

(2) CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | SYMMETRIC KEYS

Produce, control, and distribute symmetric cryptographic keys using [*Selection: NIST FIPS-compliant; NSA-approved*] key management technology and processes.

Supplemental Guidance: None.

Related Controls: None.

(3) CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | ASYMMETRIC KEYS

Produce, control, and distribute asymmetric cryptographic keys using [*Selection: NSA-approved key management technology and processes; approved DoD PKI Class 3 certificates; prepositioned keying material; approved DoD PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user's private key; certificates issued in accordance with organization-defined requirements*].

Supplemental Guidance: None.

Related Controls: None.

(4) CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | PKI CERTIFICATES
[Withdrawn: Incorporated into SC-12].

(5) CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | PKI CERTIFICATES / HARDWARE TOKENS
[Withdrawn: Incorporated into SC-12].

References: NIST Special Publications 800-56A, 800-56B, 800-56C, 800-57-1, 800-57-2, 800-57-3, 95663; NIST Interagency Reports 7956, 7966.

SC-13 CRYPTOGRAPHIC PROTECTION

Control: Implement the following cryptographic uses and type of cryptography for each use: [*Assignment: organization-defined cryptographic uses and type of cryptography required for each use*] ~~in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.~~].

Supplemental Guidance: Cryptography can be employed to support a variety of security solutions including, for example, the protection of classified information and Controlled Unclassified Information; the provision and implementation of digital signatures; and the enforcement of information separation when authorized individuals have the necessary clearances but lack the necessary formal access approvals. Cryptography can also be used to support random number generation and hash generation. Generally applicable cryptographic standards include FIPS-validated cryptography and NSA-approved cryptography. This control does not impose any requirements on organizations to use cryptography. However, if cryptography is required due to the selection of other security controls, organizations define each type of cryptographic use and the type of cryptography required ~~(e.g., protection of~~ . For example, organizations that need to protect classified information specify the use of NSA-approved cryptography. Organizations that need to provision and implement digital signatures specify the use of FIPS-validated cryptography. In all instances, cryptography is implemented in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidelines.

Related Controls: AC-2, AC-3, AC-7, AC-17, AC-18, AC-19, AU-9, AU-10, CM-11, CP-9, IA-3, IA-7, MA-4, MP-2, MP-4, MP-5, SA-4, SA-9, SC-8, SC-12, SC-20, SC-23, SC-28, SC-40, SI-3, SI-7.

Control Enhancements: None.

(1) CRYPTOGRAPHIC PROTECTION | FIPS-VALIDATED CRYPTOGRAPHY
[Withdrawn: Incorporated into SC-13].

(2) CRYPTOGRAPHIC PROTECTION | NSA-APPROVED CRYPTOGRAPHY
[Withdrawn: Incorporated into SC-13].

(3) CRYPTOGRAPHIC PROTECTION | INDIVIDUALS WITHOUT FORMAL ACCESS APPROVALS
[Withdrawn: Incorporated into SC-13].

(4) CRYPTOGRAPHIC PROTECTION | DIGITAL SIGNATURES
[Withdrawn: Incorporated into SC-13].

References: FIPS Publication 140-2.

SC-14 PUBLIC ACCESS PROTECTIONS

[Withdrawn: ~~Capability provided by~~Incorporated into AC-2, AC-3, AC-5, AC-6, SI-3, SI-4, SI-5, SI-7, SI-10].

SC-15 COLLABORATIVE COMPUTING DEVICES AND APPLICATIONS

Control:

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.

Supplemental Guidance: Collaborative computing devices and applications include, for example, remote meeting devices and applications, networked white boards, cameras, and microphones. Explicit indication of use includes, for example, signals to users when collaborative computing devices and applications are activated.

Related Controls: AC-21.

Control Enhancements:

(1) COLLABORATIVE COMPUTING DEVICES | PHYSICAL DISCONNECT

Provide physical disconnect of collaborative computing devices in a manner that supports ease of use.

Supplemental Guidance: Failing to physically disconnect from collaborative computing devices can result in subsequent compromises of organizational information. Providing easy methods to physically 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.

Related Controls: None.

(2) COLLABORATIVE COMPUTING DEVICES | BLOCKING INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC

[Withdrawn: Incorporated into SC-7].

(3) COLLABORATIVE COMPUTING DEVICES | 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*].

Supplemental Guidance: Failing to disable or remove collaborative computing devices and applications from systems or system components can result in subsequent compromises of organizational information including, for example, eavesdropping on conversations.

Related Controls: None.

(4) COLLABORATIVE COMPUTING DEVICES | EXPLICITLY INDICATE CURRENT PARTICIPANTS

Provide an explicit indication of current participants in [*Assignment: organization-defined online meetings and teleconferences*].

Supplemental Guidance: This control enhancement helps to prevent unauthorized individuals from participating in collaborative computing sessions without the explicit knowledge of other participants.

Related Controls: None.

References: None.

SC-16 TRANSMISSION OF SECURITY AND PRIVACY ATTRIBUTES

Control: ~~The information system associates~~Associate [*Assignment: organization-defined security and privacy attributes*] with information exchanged between ~~information~~ systems and between system components.

Supplemental Guidance: Security and privacy attributes can be explicitly or implicitly associated with the information contained in ~~organizational information~~ systems or system components. Attributes are an abstraction representing the basic properties or characteristics of an entity with respect to safeguarding information or the management of personally identifiable information. Attributes are typically associated with internal data structures including, for example, records, buffers, files within the information system. Security and privacy attributes are used to implement access control and flow control policies; reflect special dissemination, management, or distribution instructions, including permitted uses of personally identifiable information; or support other

aspects of the information security and privacy policies. Privacy attributes may be used independently, or in conjunction with security attributes.

Related Controls: AC-3, AC-4, AC-16.

Control Enhancements:

(1) TRANSMISSION OF SECURITY AND PRIVACY ATTRIBUTES | INTEGRITY VALIDATION

Validate the integrity of transmitted security and privacy attributes.

Supplemental Guidance: This control enhancement ensures that the integrity verification of transmitted information includes security and privacy attributes.

Related Controls: AU-10, SC-8.

References: None.

SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES

Control: Issue public key certificates under an [*Assignment: organization-defined certificate policy*] or obtain public key certificates from an approved service provider.

Supplemental Guidance: For all certificates, organizations manage system trust stores to ensure only approved trust anchors are in the trust stores. This control addresses certificates with visibility external to organizational systems and certificates related to the internal operations of systems, for example, application-specific time services.

Related Controls: AU-10, IA-5, SC-12.

Control Enhancements: None.

References: NIST Special Publications 800-32, 800-57-1, 800-57-2, 800-57-3, 800-63.

SC-18 MOBILE CODE

Control:

a. Define acceptable and unacceptable mobile code and mobile code technologies;

b. Establish usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and

c. Authorize, monitor, and control the use of mobile code within the system.

Supplemental Guidance: Decisions regarding the use of mobile code within organizational systems are based on the potential for the code to cause damage to the systems if used maliciously. Mobile code technologies include, for example, Java, JavaScript, ActiveX, Postscript, PDF, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidelines apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations and devices including, for example, notebook computers and smart phones. Mobile code policy and procedures address the specific actions taken to prevent the development, acquisition, and introduction of unacceptable mobile code within organizational systems.

Related Controls: AU-2, AU-12, CM-2, CM-6, SI-3.

Control Enhancements:

(1) MOBILE CODE | IDENTIFY UNACCEPTABLE CODE AND TAKE CORRECTIVE ACTIONS

Identify [*Assignment: organization-defined unacceptable mobile code*] and take [*Assignment: organization-defined corrective actions*].

Supplemental Guidance: Corrective actions when unacceptable mobile code is detected include, for example, blocking, quarantine, or alerting administrators. Blocking includes, for example, preventing transmission of word processing files with embedded macros when such macros have been defined to be unacceptable mobile code.

Related Controls: None.

(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*].

Supplemental Guidance: None.

Related Controls: None.

(3) MOBILE CODE | PREVENT DOWNLOADING AND EXECUTION

Prevent the download and execution of [*Assignment: organization-defined unacceptable mobile code*].

Supplemental Guidance: None.

Related Controls: None.

(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.

Supplemental Guidance: Actions enforced before executing mobile code, include, for example, prompting users prior to opening electronic mail attachments. Preventing automatic execution of mobile code includes, for example, disabling auto execute features on system components employing portable storage devices such as Compact Disks (CDs), Digital Video Disks (DVDs), and Universal Serial Bus (USB) devices.

Related Controls: None.

(5) MOBILE CODE | ALLOW EXECUTION ONLY IN CONFINED ENVIRONMENTS

Allow execution of permitted mobile code only in confined virtual machine environments.

Supplemental Guidance: None.

Related Controls: SC-44, SI-7.

References: NIST Special Publication 800-28.

SC-19 VOICE OVER INTERNET PROTOCOL

Control:

a. Establish usage restrictions and implementation guidelines for Voice over Internet Protocol (VoIP) technologies; and

b. Authorize, monitor, and control the use of VoIP technologies within the system.

Supplemental Guidance: Usage restrictions and implementation guidelines are based on the potential for the VoIP technology to cause damage to the system if used maliciously.

Related Controls: CM-6, SC-7, SC-15.

Control Enhancements: None.

References: NIST Special Publication 800-58.

SC-20 SECURE NAME/ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)

Control:

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.

Supplemental Guidance: This control enables external clients including, for example, remote Internet clients, to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service. Systems that provide name and address resolution services include, for example, domain name system (DNS) servers. Additional artifacts include, for example, DNS Security (DNSSEC) digital signatures and cryptographic keys. DNS resource records are examples of authoritative data. The means to indicate the security status of child zones includes, for example, the use of delegation signer resource records in the DNS. ~~The DNS security controls reflect (and are referenced from) OMB Memorandum 08-23. Information~~ Systems that use technologies other than the DNS to map between host and service names and network addresses provide other means to assure the authenticity and integrity of response data.

Related Controls: AU-10, SC-8, SC-12, SC-13, SC-21, SC-22.

Control Enhancements:

(1) SECURE NAME/ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) | CHILD SUBSPACES
[Withdrawn: Incorporated into 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.

Supplemental Guidance: None.

Related Controls: None.

References: FIPS Publications 140-2, 186-4; NIST Special Publication 800-81.

SC-21 SECURE NAME/ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)

Control: Request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

Supplemental Guidance: Each client of name resolution services either performs this validation on its own, or has authenticated channels to trusted validation providers. Systems that provide name and address resolution services for local clients include, for example, recursive resolving or caching domain name system (DNS) servers. DNS client resolvers either perform validation of DNSSEC signatures, or clients use authenticated channels to recursive resolvers that perform such validations. Systems that use technologies other than the DNS to map between host/service names and network addresses provide some other means to enable clients to verify the authenticity and integrity of response data.

Related Controls: SC-20, SC-22.

Control Enhancements: None.

(1) SECURE NAME/ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER) | DATA ORIGIN AND INTEGRITY
[Withdrawn: Incorporated into SC-21].

References: NIST Special Publication 800-81.

SC-22 ARCHITECTURE AND PROVISIONING FOR NAME/ADDRESS RESOLUTION SERVICE

Control: Ensure the systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal and external role separation.

Supplemental Guidance: Systems that provide name and address resolution services include, for example, domain name system (DNS) servers. To eliminate single points of failure and to enhance redundancy, organizations employ at least two authoritative domain name system servers; one configured as the primary server and the other configured as the secondary server. Additionally, organizations typically deploy the servers in two geographically separated network subnetworks (i.e., not located in the same physical facility). For role separation, DNS servers with internal roles only process name and address resolution requests from within organizations (i.e., from internal

clients). DNS servers with external roles only process name and address resolution information requests from clients external to organizations (i.e., on external networks including the Internet). Organizations specify clients that can access authoritative DNS servers in certain roles, for example, by address ranges and explicit lists.

Related Controls: SC-2, SC-20, SC-21, SC-24.

Control Enhancements: None.

References: NIST Special Publication 800-81.

SC-23 SESSION AUTHENTICITY

Control: Protect the authenticity of communications sessions.

Supplemental Guidance: This control addresses communications protection at the session, versus packet level ~~(e.g., sessions in service-oriented architectures providing web-based services) and.~~ Such protection establishes grounds for confidence at both ends of communications sessions in the ongoing identities of other parties and in the validity of information transmitted. Authenticity protection includes, for example, protecting against man-in-the-middle attacks and session hijacking, and the insertion of false information into sessions.

Related Controls: AU-10, SC-8, SC-10, SC-11.

Control Enhancements:

(1) SESSION AUTHENTICITY | INVALIDATE SESSION IDENTIFIERS AT LOGOUT

Invalidate session identifiers upon user logout or other session termination.

Supplemental Guidance: This control enhancement curtails the ability of adversaries from capturing and continuing to employ previously valid session IDs.

Related Controls: None.

(2) SESSION AUTHENTICITY | USER-INITIATED LOGOUTS AND MESSAGE DISPLAYS

[Withdrawn: Incorporated into AC-12(1)].

(3) SESSION AUTHENTICITY | UNIQUE SESSION IDENTIFIERS WITH RANDOMIZATION

Generate a unique session identifier for each session with [*Assignment: organization-defined randomness requirements*] and recognize only session identifiers that are system-generated.

Supplemental Guidance: This control enhancement curtails the ability of adversaries from reusing previously valid session IDs. Employing the concept of randomness in the generation of unique session identifiers protects against brute-force attacks to determine future session identifiers.

Related Controls: AC-10, SC-13.

(4) SESSION AUTHENTICITY | UNIQUE SESSION IDENTIFIERS WITH RANDOMIZATION

[Withdrawn: Incorporated into SC-23(3)].

(5) SESSION AUTHENTICITY | ALLOWED CERTIFICATE AUTHORITIES

Only allow the use of [*Assignment: organization-defined certificate authorities*] for verification of the establishment of protected sessions.

Supplemental Guidance: Reliance on certificate authorities (CAs) for the establishment of secure sessions includes, for example, the use of ~~Secure Socket Layer (SSL) and/or~~ Transport Layer Security (TLS) certificates. These certificates, after verification by their respective CAs, facilitate the establishment of protected sessions between web clients and web servers.

Related Controls: SC-13.

References: NIST Special Publications 800-52, 800-77, 800-95, 800-113.

SC-24 FAIL IN KNOWN STATE

Control: Fail to a [*Assignment: organization-defined known system state*] for [*Assignment: organization-defined types of system failures*] preserving [*Assignment: organization-defined system state information*] in failure.

Supplemental Guidance: Failure in a known state addresses security concerns in accordance with the mission and business needs of organizations. Failure in a known state helps to prevent the loss of confidentiality, integrity, or availability of information in the event of failures of organizational systems or system components. Failure in a known safe state helps to prevent systems from failing to a state that may cause injury to individuals or destruction to property. Preserving system state information facilitates system restart and return to the operational mode of organizations with less disruption of mission and business processes.

Related Controls: CP-2, CP-4, CP-10, CP-12, SC-7, SC-22, SI-13.

Control Enhancements: None.

References: None.

SC-25 THIN NODES

Control: Employ [*Assignment: organization-defined system components*] with minimal functionality and information storage.

Supplemental Guidance: The deployment of system components with ~~reduced/~~minimal functionality ~~(e.g., diskless nodes and thin client technologies)~~ reduces the need to secure every user endpoint, and may reduce the exposure of information, systems, and services to ~~cyber~~ attacks. Examples of reduced or minimal functionality include, for example, diskless nodes and thin client technologies.

Related Controls: SC-30, SC-44.

Control Enhancements: None.

References: None.

SC-26 HONEYPOTS

Control: Include components within organizational systems specifically designed to be the target of malicious attacks for detecting, deflecting, and analyzing such attacks.

Supplemental Guidance: A honeypot is established as a decoy to attract adversaries and to deflect their attacks away from the operational systems supporting organizational missions and business functions. Depending upon the specific usage of the honeypot, consultation with the Office of the General Counsel before deployment may be needed.

Related Controls: SC-30, SC-35, SC-44, SI-3, SI-4.

Control Enhancements: None.

(1) HONEYPOTS | DETECTION OF MALICIOUS CODE
[Withdrawn: Incorporated into SC-35].

References: None.

SC-27 PLATFORM-INDEPENDENT APPLICATIONS

Control: Include within organizational systems: [*Assignment: organization-defined platform-independent applications*].

Supplemental Guidance: Platforms are combinations of hardware and software used to run software applications. Platforms include operating systems; the underlying computer architectures; or both. Platform-independent applications are those applications with the capability to execute on multiple platforms. Such applications promote portability and reconstitution on different platforms. This

increases the availability of critical or essential functions within organizations in situations where systems with specific operating systems are under attack.

Related Controls: SC-29.

Control Enhancements: None.

References: None.

SC-28 PROTECTION OF INFORMATION AT REST

Control: Protect the [*Selection (one or more): confidentiality; integrity*] of [*Assignment: organization-defined information*] at rest.

Supplemental Guidance: This control addresses the confidentiality and integrity of information at rest and covers user information and system information. Information at rest refers to the state of information when it is not in process or in transit and is located on storage devices as specific components of systems. The focus of this control is not on the type of storage device or frequency of access but rather the state of the information. System-related information requiring protection includes, for example, configurations or rule sets for firewalls, gateways, intrusion detection and prevention systems, filtering routers, and authenticator content. Organizations may employ different mechanisms to achieve confidentiality and integrity protections, including the use of cryptographic mechanisms and file share scanning. Integrity protection can be achieved, for example, by implementing Write-Once-Read-Many (WORM) technologies. When adequate protection of information at rest cannot otherwise be achieved, organizations may employ other security controls including, for example, frequent scanning to identify malicious code at rest and secure off-line storage in lieu of online storage ~~when adequate protection of information at rest cannot otherwise be achieved and/or continuous monitoring to identify malicious code at rest.~~ .

Related Controls: AC-3, AC-6, AC-19, CA-7, CM-3, CM-5, CM-6, CP-9, MP-4, MP-5, PE-3, SC-8, SC-13, SC-34, SI-3, SI-7, SI-16.

Control Enhancements:

(1) PROTECTION OF INFORMATION AT REST | CRYPTOGRAPHIC PROTECTION

Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of [*Assignment: organization-defined information*] when at rest on [*Assignment: organization-defined system components*].

Supplemental Guidance: ~~Selection of cryptographic mechanisms is based on the need to protect the confidentiality and integrity of organizational information. The strength of mechanism is commensurate with the security category and/or classification of the information.~~ This control enhancement applies to significant concentrations of digital media in organizational areas designated for media storage. It also applies to limited quantities of media generally associated with system components in operational environments including, for example, portable storage devices, notebook computers, and mobile devices. Selection of cryptographic mechanisms is based on the need to protect the confidentiality and integrity of organizational information. The strength of mechanism is commensurate with the security category or classification of the information. Organizations have the flexibility to ~~either~~ encrypt all information on storage devices ~~(i.e., full disk encryption)~~ or encrypt specific data structures ~~(e.g.,~~including, for example, files, records, or fields. Organizations employing cryptographic mechanisms to protect information at rest also consider cryptographic key management solutions.

Related Controls: AC-19, SC-12.

(2) PROTECTION OF INFORMATION AT REST | OFF-LINE STORAGE

Remove the following information from online storage and store off-line in a secure location: [*Assignment: organization-defined information*].

Supplemental Guidance: Removing organizational information from online system storage to off-line storage eliminates the possibility of individuals gaining unauthorized access to the

information through a network. Therefore, organizations may choose to move information to off-line storage in lieu of protecting such information in online storage.

Related Controls: None.

References: NIST Special Publications 800-56A, 800-56B, 800-56C, 800-57-1, 800-57-2, 800-57-3, 800-111, 800-124.

SC-29 HETEROGENEITY

Control: Employ a diverse set of information technologies for [*Assignment: organization-defined system components*] in the implementation of the system.

Supplemental Guidance: Increasing the diversity of information technologies within organizational systems reduces the impact of potential exploitations or compromises of specific technologies ~~and also defends~~. Such diversity protects against common mode failures, including those failures induced by supply chain attacks. Diversity in information technologies also reduces the likelihood that the means adversaries use to compromise one system component will be equally effective against other system components, thus further increasing the adversary work factor to successfully complete planned attacks. An increase in diversity may add complexity and management overhead which could ultimately lead to mistakes and unauthorized configurations.

Related Controls: AU-9, PL-8, SA-12, SC-27, SC-30.

Control Enhancements:

~~(2)~~(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*].

Supplemental Guidance: While frequent changes to operating systems and applications pose 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.

Related Controls: None.

References: None.

SC-30 CONCEALMENT AND MISDIRECTION

Control: Employ [*Assignment: organization-defined concealment and misdirection techniques*] for [*Assignment: organization-defined systems*] at [*Assignment: organization-defined time-periods*] to confuse and mislead adversaries.

Supplemental Guidance: Concealment and misdirection techniques can significantly reduce the targeting capability of adversaries (i.e., window of opportunity and available attack surface) to initiate and complete attacks. For example, virtualization techniques provide organizations with the ability to disguise systems, potentially reducing the likelihood of successful attacks without the cost of having multiple platforms. Increased use of concealment and misdirection techniques and methods including, for example, randomness, uncertainty, and virtualization, may sufficiently confuse and mislead adversaries and subsequently increase the risk of discovery and/or exposing tradecraft. Concealment and misdirection techniques may also provide organizations additional time to successfully perform core missions and business functions. Because of the time and effort required to support concealment and misdirection techniques, it is anticipated that such techniques would be used by organizations on a very limited basis.

Related Controls: AC-6, SC-25, SC-26, SC-29, SC-44, SI-14.

Control Enhancements:

(1) CONCEALMENT AND MISDIRECTION | VIRTUALIZATION TECHNIQUES

[Withdrawn: Incorporated into SC-29(1)].

(2) CONCEALMENT AND MISDIRECTION | RANDOMNESS

Employ [*Assignment: organization-defined techniques*] to introduce randomness into organizational operations and assets.

Supplemental Guidance: Randomness introduces increased levels of uncertainty for adversaries regarding the actions organizations take in defending their systems against attacks. Such actions may impede the ability of adversaries to correctly target information resources of organizations supporting critical missions or business functions. Uncertainty may also cause adversaries to hesitate before initiating or continuing their attacks. Misdirection techniques involving randomness include, for example, performing certain routine actions at different times of day, employing different information technologies ~~(e.g., browsers, search engines),~~ using different suppliers, and rotating roles and responsibilities of organizational personnel.

Related Controls: None.

(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*]].

Supplemental Guidance: Adversaries target critical ~~organizational~~ missions and business functions and the ~~information resources~~systems supporting those missions and functions while at the same time, trying to minimize exposure of their existence and tradecraft. The static, homogeneous, and deterministic nature of organizational systems targeted by adversaries, make such systems more susceptible to ~~cyber~~ attacks with less adversary cost and effort to be successful. Changing ~~organizational~~ processing and storage locations (sometimes referred to as moving target defense) addresses the advanced persistent threat (APT) using techniques such as virtualization, distributed processing, and replication. This enables organizations to relocate the ~~information resources~~system components (i.e., processing and/or storage) supporting critical missions and business functions. Changing the locations of processing activities and/or storage sites introduces a degree of uncertainty into the targeting activities by adversaries. This uncertainty increases the work factor of adversaries making compromises or breaches to organizational systems much more difficult and time-consuming. It also increases the chances that adversaries may inadvertently disclose aspects of tradecraft while attempting to locate critical organizational resources.

Related Controls: None.

(4) CONCEALMENT AND MISDIRECTION | MISLEADING INFORMATION

Employ realistic, but misleading information in [*Assignment: organization-defined system components*] about its security state or posture.

Supplemental Guidance: This control enhancement misleads potential adversaries regarding the nature and extent of security safeguards deployed by organizations. Thus, adversaries may employ incorrect and ineffective, attack techniques. One way of misleading adversaries is for organizations to place misleading information regarding the specific ~~security~~ controls deployed in external systems that are known to be ~~accessed or~~ targeted by adversaries. Another technique is the use of deception nets ~~(e.g., honeynets, virtualized environments)~~ that mimic actual aspects of organizational systems but use, for example, out-of-date software configurations.

Related Controls: None.

(5) CONCEALMENT AND MISDIRECTION | CONCEALMENT OF SYSTEM COMPONENTS

Employ [*Assignment: organization-defined techniques*] to hide or conceal [*Assignment: organization-defined system components*].

Supplemental Guidance: By hiding, disguising, or ~~otherwise~~ concealing critical ~~information~~ system components, organizations may be able to decrease the probability that adversaries target and successfully compromise those assets. Potential means for organizations to hide, disguise, or conceal system components include, for example, configuration of routers or the use of honeynets or virtualization techniques.

Related Controls: None.

References: None.

SC-31 COVERT CHANNEL ANALYSIS

Control:

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.

Supplemental Guidance: Developers are in the best position to identify potential areas within systems that might lead to covert channels. Covert channel analysis is a meaningful activity when there is the potential for unauthorized information flows across handling caveats, discretionary policies, or security domains, for example, in the case of systems containing export-controlled information and having connections to external networks (i.e., networks that are not controlled by organizations). Covert channel analysis is also ~~meaningful~~useful for multilevel secure systems, multiple security level systems, and cross-domain systems.

Related Controls: AC-3, AC-4, SI-11.

Control Enhancements:

(1) COVERT CHANNEL ANALYSIS | TEST COVERT CHANNELS FOR EXPLOITABILITY

Test a subset of the identified covert channels to determine which channels are exploitable.

Supplemental Guidance: None.

Related Controls: None.

(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*].

Supplemental Guidance: ~~Information system developers are in the best position to reduce the maximum bandwidth for identified covert storage and timing channels~~None.

Related Controls: None.

(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.

Supplemental Guidance: This control enhancement addresses covert channel bandwidth in operational environments versus developmental environments. Measuring covert channel bandwidth in specified operational environments helps organizations to determine how much information can be covertly leaked before such leakage adversely affects missions or business functions. Covert channel bandwidth may be significantly different when measured in those settings that are independent of the specific environments of operation including, for example, laboratories or development environments.

Related Controls: None.

References: None.

SC-32 SYSTEM PARTITIONING

Control: Partition the system into [*Assignment: organization-defined system components*] residing in separate physical domains or environments based on [*Assignment: organization-defined circumstances for physical separation of components*].

Supplemental Guidance: System partitioning is a part of a defense-in-depth protection strategy. Organizations determine the degree of physical separation of system components from physically distinct components in separate racks in the same room, to components in separate rooms for the

more critical components, to significant geographical separation of the most critical components. Security categorization can guide the selection of appropriate candidates for domain partitioning. Managed interfaces restrict or prohibit network access and information flow among partitioned system components.

Related Controls: AC-4, AC-6, SA-8, SC-2, SC-3, SC-7, SC-36.

Control Enhancements: None.

References: FIPS Publication 199.

SC-33 TRANSMISSION PREPARATION INTEGRITY

[Withdrawn: Incorporated into SC-8].

SC-34 NON-MODIFIABLE EXECUTABLE PROGRAMS

Control: At [*Assignment: organization-defined system components*]:

a. Load and execute the operating environment from hardware-enforced, read-only media; and

b. Load and execute [*Assignment: organization-defined applications*] from hardware-enforced, read-only media.

Supplemental Guidance: The operating environment for a system contains the specific code that hosts applications, for example, operating systems, executives, or monitors including virtual machine monitors (i.e., hypervisors). It can also include certain applications running directly on hardware platforms. Hardware-enforced, read-only media include, for example, Compact Disk-Recordable (CD-R) and Digital Video Disk-Recordable (DVD-R) disk drives and one-time programmable read-only memory. The use of non-modifiable storage ensures the integrity of software from the point of creation of the read-only image. The use of reprogrammable read-only memory can be accepted as read-only media provided integrity can be adequately protected from the point of initial writing to the insertion of the memory into the system; and there are reliable hardware protections against reprogramming the memory while installed in organizational systems.

Related Controls: AC-3, SI-7, SI-14.

Control Enhancements:

(1) NON-MODIFIABLE EXECUTABLE PROGRAMS | NO WRITABLE STORAGE

Employ [*Assignment: organization-defined system components*] with no writeable storage that is persistent across component restart or power on/off.

Supplemental Guidance: This control enhancement eliminates the possibility of malicious code insertion via persistent, writeable storage within the designated system components. It applies to fixed and removable storage, with the latter being addressed either directly or as specific restrictions imposed through access controls for mobile devices.

Related Controls: AC-19, MP-7.

(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 after such information has been recorded onto the media.

Supplemental Guidance: Security safeguards prevent the substitution of media into systems or the reprogramming of programmable read-only media prior to installation into the systems. Such safeguards include, for example, a combination of prevention, detection, and response.

Related Controls: CM-3, CM-5, CM-9, MP-2, MP-4, MP-5, SC-28, SI-3.

(3) NON-MODIFIABLE EXECUTABLE PROGRAMS | 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.

Supplemental Guidance: None.

Related Controls: None.

References: None.

SC-35 HONEYCLIENTS

Control: Include system components that proactively seek to identify network-based malicious code, malicious websites, or web-based malicious code.

Supplemental Guidance: Honeyclients differ from honeypots in that the components actively probe networks including, the Internet, in search of malicious code ~~(e.g., worms)~~ contained on external websites. Like honeypots, honeyclients require some supporting isolation measures ~~(e.g., virtualization)~~ to ensure that any malicious code discovered during the search and subsequently executed does not infect organizational systems. Virtualization is a common technique for achieving such isolation.

Related Controls: SC-26, SC-44, SI-3, SI-4.

Control Enhancements: None.

References: None.

SC-36 DISTRIBUTED PROCESSING AND STORAGE

Control: Distribute [*Assignment: organization-defined processing and storage components*] across multiple physical locations.

Supplemental Guidance: Distributing processing and storage across multiple physical locations provides some degree of redundancy or overlap for organizations, and therefore increases the work factor of adversaries to adversely impact organizational operations, assets, and individuals. This control does not assume a single primary processing or storage location, and therefore, allows for parallel processing and storage.

Related Controls: CP-6, CP-7, PL-8, SC-32.

Control Enhancements:

(1) DISTRIBUTED PROCESSING AND STORAGE | POLLING TECHNIQUES

(a) Employ polling techniques to identify potential faults, errors, or compromises to [*Assignment: organization-defined distributed processing and storage components*]; and

(b) Take [*Assignment: organization-defined action*] in response to identified faults, errors, or compromises.

Supplemental Guidance: Distributed processing and/or storage may be employed to reduce opportunities for adversaries to successfully compromise the confidentiality, integrity, or availability of information and systems. However, distribution of processing and/or storage components does not prevent adversaries from compromising one (or more) of the distributed components. Polling compares the processing results and/or storage content from the various distributed components and subsequently voting on the outcomes. Polling identifies potential faults, errors, or compromises in distributed processing and storage components. Polling techniques may also be applied to processing and storage components that are not physically distributed.

Related Controls: SI-4.

References: None.

SC-37 OUT-OF-BAND CHANNELS

Control: Employ [*Assignment: organization-defined out-of-band channels*] for the physical delivery or electronic transmission of [*Assignment: organization-defined information, system components, or devices*] to [*Assignment: organization-defined individuals or systems*].

Supplemental Guidance: Out-of-band channels include, for example, local nonnetwork accesses to systems; network paths physically separate from network paths used for operational traffic; or nonelectronic paths such as the US Postal Service. This is in contrast with using the same channels (i.e., in-band channels) that carry routine operational traffic. Out-of-band channels do not have the same vulnerability or exposure as in-band channels, and therefore, the confidentiality, integrity, or availability compromises of in-band channels will not compromise or adversely affect the out-of-band channels. Organizations may employ out-of-band channels in the delivery or transmission of many organizational items including, for example, identifiers and authenticators; cryptographic key management information; configuration management changes for hardware, firmware, or software; security updates; system and data backups; maintenance information; and malicious code protection updates.

Related Controls: AC-2, CM-3, CM-5, CM-7, IA-2, IA-4, IA-5, MA-4, SC-12, SI-3, SI-4, SI-7.

Control Enhancements:

(1) OUT-OF-BAND CHANNELS | ENSURE DELIVERY AND TRANSMISSION

Employ [*Assignment: organization-defined security safeguards*] to ensure that only [*Assignment: organization-defined individuals or systems*] receive the [*Assignment: organization-defined information, system components, or devices*].

Supplemental Guidance: Techniques employed by organizations to ensure that only designated systems or individuals receive ~~particular~~certain information, system components, or devices include, for example, sending authenticators via an approved courier service but requiring recipients to show some form of government-issued photographic identification as a condition of receipt.

Related Controls: None.

References: NIST Special Publication 800-57-1, 800-57-2, 800-57-3.

SC-38 OPERATIONS SECURITY

Control: Employ [*Assignment: organization-defined operations security safeguards*] to protect key organizational information throughout the system development life cycle.

Supplemental Guidance: Operations security (OPSEC) is a systematic process by which potential adversaries can be denied information about the capabilities and intentions of organizations by identifying, controlling, and protecting generally unclassified information that specifically relates to the planning and execution of sensitive organizational activities. The OPSEC process involves five steps: identification of critical information ~~(e.g., the security categorization process~~; analysis of threats; analysis of vulnerabilities; assessment of risks; and the application of appropriate countermeasures. OPSEC safeguards are applied to organizational systems and the environments in which those systems operate. OPSEC safeguards protect the confidentiality of key information including, for example, limiting the sharing of information with suppliers and potential suppliers of system components~~, information technology products~~ and services, and with other non-organizational elements and individuals. Information critical to organizational mission and business success includes, for example, user identities, element uses, suppliers, supply chain processes, functional and security requirements, system design specifications, testing and evaluation protocols, and security control implementation details.

Related Controls: CA-2, CA-7, PL-1, PM-9, PM-12, RA-2, RA-3, RA-5, SA-12, SC-7.

Control Enhancements: None.

References: None.

SC-39 PROCESS ISOLATION

Control: Maintain a separate execution domain for each executing process with the system.

Supplemental Guidance: Systems can maintain separate execution domains for each executing process by assigning each process a separate address space. Each system process has a distinct address space so that communication between processes is performed in a manner controlled through the security functions, and one process cannot modify the executing code of another process. Maintaining separate execution domains for executing processes can be achieved, for example, by implementing separate address spaces. This capability is readily available in most commercial operating systems that employ multi-state processor technologies.

Related Controls: AC-3, AC-4, AC-6, AC-25, SA-8, SC-2, SC-3.

Control Enhancements:

(1) PROCESS ISOLATION | HARDWARE SEPARATION

Implement hardware separation mechanisms to facilitate process separation.

Supplemental Guidance: 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, for example, hardware memory management.

Related Controls: None.

(2) PROCESS ISOLATION | THREAD ISOLATION

Maintain a separate execution domain for each thread in [*Assignment: organization-defined multi-threaded processing*].

Supplemental Guidance: None.

Related Controls: None.

References: None.

SC-40 WIRELESS LINK PROTECTION

Control: Protect external and internal [*Assignment: organization-defined wireless links*] from [*Assignment: organization-defined types of signal parameter attacks or references to sources for such attacks*].

Supplemental Guidance: This control applies to internal and external wireless communication links that may be visible to individuals who are not authorized system users. Adversaries can exploit the signal parameters of wireless links if such links are not adequately protected. There are many ways to exploit the signal parameters of wireless links to gain intelligence, deny service, or spoof users of organizational systems. This control reduces the impact of attacks that are unique to wireless systems. If organizations rely on commercial service providers for transmission services as commodity items rather than as fully dedicated services, it may not be possible to implement this control.

Related Controls: AC-18, SC-5.

Control Enhancements:

(1) WIRELESS LINK PROTECTION | ELECTROMAGNETIC INTERFERENCE

Implement cryptographic mechanisms that achieve [*Assignment: organization-defined level of protection*] against the effects of intentional electromagnetic interference.

Supplemental Guidance: This control enhancement protects against intentional jamming that might deny or impair communications by ensuring that wireless spread spectrum waveforms used to provide anti-jam protection are not predictable by unauthorized individuals. The control enhancement may also coincidentally help to mitigate the effects of unintentional jamming due to interference from legitimate transmitters sharing the same spectrum. Mission requirements, projected threats, concept of operations, and applicable legislation, directives,

regulations, policies, standards, and guidelines determine levels of wireless link availability and performance/cryptography needed.

Related Controls: SC-12, SC-13.

(2) WIRELESS LINK PROTECTION | REDUCE DETECTION POTENTIAL

Implement cryptographic mechanisms to reduce the detection potential of wireless links to [*Assignment: organization-defined level of reduction*].

Supplemental Guidance: This control enhancement is needed for covert communications and protecting wireless transmitters from being geo-located by their transmissions. The control enhancement ensures that spread spectrum waveforms used to achieve low probability of detection are not predictable by unauthorized individuals. Mission requirements, projected threats, concept of operations, and applicable legislation, directives, regulations, policies, standards, and guidelines determine the levels to which wireless links should be undetectable.

Related Controls: SC-12, SC-13.

(3) WIRELESS LINK PROTECTION | IMITATIVE OR MANIPULATIVE COMMUNICATIONS DECEPTION

Implement cryptographic mechanisms to identify and reject wireless transmissions that are deliberate attempts to achieve imitative or manipulative communications deception based on signal parameters.

Supplemental Guidance: This control enhancement ensures that the signal parameters of wireless transmissions are not predictable by unauthorized individuals. Such unpredictability reduces the probability of imitative or manipulative communications deception based upon signal parameters alone.

Related Controls: SC-12, SC-13, SI-4.

(4) WIRELESS LINK PROTECTION | SIGNAL PARAMETER IDENTIFICATION

Implement cryptographic mechanisms to prevent the identification of [*Assignment: organization-defined wireless transmitters*] by using the transmitter signal parameters.

Supplemental Guidance: Radio fingerprinting techniques identify the unique signal parameters of transmitters to fingerprint such transmitters for purposes of tracking and mission/user identification. This control enhancement protects against the unique identification of wireless transmitters for purposes of intelligence exploitation by ensuring that anti-fingerprinting alterations to signal parameters are not predictable by unauthorized individuals. This control enhancement helps assure mission success when anonymity is required.

Related Controls: SC-12, SC-13.

References: None.

SC-41 PORT AND I/O DEVICE ACCESS

Control: ~~physically disables~~[*Selection: Physically* or ~~removes~~*Logically*] disable or remove [*Assignment: organization-defined connection ports or input/output devices*] on [*Assignment: organization-defined systems or system components*].

Supplemental Guidance: Connection ports include, for example, Universal Serial Bus (USB) and Firewire (IEEE 1394). Input/output (I/O) devices include, for example, Compact Disk (CD) and Digital Video Disk (DVD) drives. ~~Physically~~ Disabling or removing such connection ports and I/O devices helps prevent exfiltration of information from systems and the introduction of malicious code into systems from those ports or devices. Physically disabling or removing ports and/or devices is the stronger action.

Related Controls: AC-20, MP-7.

Control Enhancements: None.

References: None.

SC-42 SENSOR CAPABILITY AND DATA

Control:

a. Prohibit 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 class of users*].

Supplemental Guidance: This control often applies to types of systems or system components characterized as mobile devices, for example, smart phones, tablets, and E-readers. These systems often include sensors that can collect and record data regarding the environment where the system is in use. Sensors that are embedded within mobile devices include, for example, cameras, microphones, Global Positioning System (GPS) mechanisms, and accelerometers. While the sensors on mobiles devices provide an important function, if activated covertly, such devices can potentially provide a means for adversaries to learn valuable information about individuals and organizations. For example, remotely activating the GPS function on a mobile device could provide an adversary with the ability to track the specific movements of an individual.

Related Controls: None.

Control Enhancements:

(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.

Supplemental Guidance: 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.

Related Controls: None.

(2) SENSOR CAPABILITY AND DATA | AUTHORIZED USE

Employ [*Assignment: organization-defined measures*] so that data or information collected by [*Assignment: organization-defined sensors*] is only used for authorized purposes.

Supplemental Guidance: Information collected by sensors for a specific authorized purpose could be misused for some unauthorized purpose. For example, GPS sensors that are used to support traffic navigation could be misused to track movements of individuals. Measures to mitigate such activities include, for example, additional training to ensure that authorized individuals do not abuse their authority; and in the case where sensor data or information is maintained by external parties, contractual restrictions on the use of such data/information.

Related Controls: PA-2.

(3) SENSOR CAPABILITY AND DATA | PROHIBIT USE OF DEVICES

Prohibit the use of devices possessing [*Assignment: organization-defined environmental sensing capabilities*] in [*Assignment: organization-defined facilities, areas, or systems*].

Supplemental Guidance: For example, organizations may prohibit individuals from bringing cell phones or digital cameras into certain designated facilities or controlled areas within facilities where classified information is stored or sensitive conversations are taking place.

Related Controls: None.

(4) SENSOR CAPABILITY AND DATA | NOTICE OF COLLECTION

Employ the following measures to facilitate an individual's awareness that personally identifiable information is being collected by [*Assignment: organization-defined sensors*]: [*Assignment: organization-defined measures*].

Supplemental Guidance: Awareness that organizational sensors are collecting data enable individuals to more effectively engage in managing their privacy. Measures can include, for example, conventional written notices and sensor configurations that make individuals aware directly or indirectly through other devices that the sensor is collecting information. Usability and efficacy of the notice are important considerations.

Related Controls: IP-1, IP-2, IP-4.

(5) SENSOR CAPABILITY AND DATA | COLLECTION MINIMIZATION

Employ [*Assignment: organization-defined sensors*] that are configured to minimize the collection of information about individuals that is not needed.

Supplemental Guidance: Although policies to control for authorized use can be applied to information once it is collected, minimizing the collection of information that is not needed mitigates privacy-related risk at the system entry point and mitigates the risk of policy control failures. Sensor configurations include, for example, the obscuring of human features such as blurring or pixelating flesh tones.

Related Controls: None.

References: NIST Special Publication 800-124.

SC-43 USAGE RESTRICTIONS

Control:

a. Establish usage restrictions and implementation guidelines for [*Assignment: organization-defined system components*~~] based on the potential to cause damage to the information system if used maliciously;~~]; and

b. Authorize, monitor, and control the use of such components within the system.

Supplemental Guidance: This control applies to all system components ~~include hardware, software, or firmware~~including wired and wireless peripheral components ~~(e.g., Voice Over Internet Protocol, mobile code, digital~~, for example, copiers, printers, scanners, optical devices, ~~wireless~~ and other similar technologies. Usage restrictions and implementation guidelines are based on the potential for the system components to cause damage to the system if used maliciously. Usage restrictions for other technologies such as VoIP, mobile code, mobile devices, and wireless are addressed in SC-19, SC-18, AC-19, and AC-18.

Related Controls: AC-18, AC-19, CM-6, SC-7, SC-18, SC-19.

Control Enhancements: None.

References: NIST Special Publication 800-124.

SC-44 DETONATION CHAMBERS

Control: Employ a detonation chamber capability within [*Assignment: organization-defined system, system component, or location*].

Supplemental Guidance: Detonation chambers, also known as dynamic execution environments, allow organizations to open email attachments, execute untrusted or suspicious applications, and execute Universal Resource Locator requests in the safety of an isolated environment or a virtualized sandbox. These protected and isolated execution environments provide a means of determining whether the associated attachments or applications contain malicious code. While related to the concept of deception nets, this control is not intended to maintain a long-term environment in which adversaries can operate and their actions can be observed. Rather, it is intended to quickly identify malicious code and reduce the likelihood that the code is propagated to user environments of operation or prevent such propagation completely.

Related Controls: SC-7, SC-25, SC-26, SC-30, SC-35, SI-3, SI-7.

Control Enhancements: None.

References: NIST Special Publication 800-177.

3.20 SYSTEM AND INFORMATION INTEGRITY

Quick link to System and Information Integrity summary table

SI-1 SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES

Control:

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

1. A 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 senior management official*] to manage the system and information integrity policy and procedures;

~~b.~~c. Review and update the current system and information integrity:

1. Policy [*Assignment: organization-defined frequency*]; and

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

d. Ensure that the system and information integrity procedures implement the system and information integrity policy and controls; and

e. Develop, document, and implement remediation actions for violations of the system and information integrity policy.

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of ~~selected security~~ the controls and control enhancements in the SI family. The risk management strategy is an important factor in establishing policy and procedures ~~reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards,~~. Comprehensive policy and ~~guidance.~~procedures help provide security and privacy assurance. Security and privacy program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general ~~information~~ security and privacy policy ~~for organizations~~ or ~~conversely,~~ can be represented by multiple policies reflecting the complex nature of ~~certain~~ organizations. The procedures can be established for security ~~program in general~~and privacy programs and for ~~particular information~~ systems, if needed. Procedures describe how policies or controls are implemented and can be directed at the personnel 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. It is important to recognize that restating controls does not constitute an organizational ~~risk management strategy is a key factor in establishing policy and procedures.~~ policy or procedure.

Related Controls: PM-9, PS-8, SI-12.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

SI-2 FLAW REMEDIATION

Control:

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.

Supplemental Guidance: 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 software updates include, for example, patches, service packs, hot fixes, and anti-virus signatures. Organizations also address flaws discovered during ~~security~~ assessments, continuous monitoring, incident response activities, and system error handling. ~~Organizations take advantage of available resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases in remediating flaws discovered in organizational information systems.~~ By incorporating flaw remediation into ongoing configuration management processes, required~~/anticipated~~ remediation actions can be tracked and verified. ~~Flaw remediation actions that can be tracked and verified include, for example, determining whether organizations follow US-CERT guidance and Information Assurance Vulnerability Alerts.~~ Organization-defined time-periods for updating security-relevant software and firmware may vary based on a variety of factors including, for example, the security category of the system or the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw). Some types of flaw remediation may require more testing than other types. Organizations determine the ~~degree and~~ type of testing needed for the specific type of flaw remediation activity under consideration and the types of changes that are to be configuration-managed. In some situations, organizations may determine that testing of software or firmware updates is not necessary or practical, for example, when implementing simple anti-virus signature updates. Organizations also consider in testing decisions, whether security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures.

Related Controls: CA-4, CM-3, CM-4, CM-5, CM-6, CM-8, MA-2, RA-5, SA-10, SA-11, SI-3, SI-5, SI-7, SI-11.

Control Enhancements:

(1) FLAW REMEDIATION | CENTRAL MANAGEMENT

Centrally manage the flaw remediation process.

Supplemental Guidance: Central management is the organization-wide management and implementation of flaw remediation processes. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed flaw remediation controls.

Related Controls: PL-9.

(2) FLAW REMEDIATION | AUTOMATED FLAW REMEDIATION STATUS

Employ automated mechanisms [*Assignment: organization-defined frequency*] to determine the state of system components with regard to flaw remediation.

Supplemental Guidance: None.

Related Controls: SI-4.

(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 [*Assignment: organization-defined benchmarks*] for taking corrective actions.

Supplemental Guidance: This control enhancement requires organizations to determine the time it takes on the 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.

Related Controls: None.

(4) FLAW REMEDIATION | AUTOMATED PATCH MANAGEMENT TOOLS

[Withdrawn: Incorporated into 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*].

Supplemental Guidance: 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.

Related Controls: None.

(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.

Supplemental Guidance: 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 ~~information technology~~ products may remove previous versions of software and firmware automatically from the system.

Related Controls: None.

(7) FLAW REMEDIATION | PERSONALLY IDENTIFIABLE INFORMATION

(a) Identify and correct flaws related to the collection, usage, processing, or dissemination of personally identifiable information;

(b) Report flaws related to personally identifiable information to the Senior Agency Official for Privacy;

(c) Receive approval for correction of privacy-related flaws from the Senior Agency Official for Privacy;

(d) Prior to installation, assess software and firmware updates related to flaw remediation for effectiveness and consistency with terms agreed upon in the privacy impact assessment;

(e) Install privacy-relevant software and firmware updates within [*Assignment: organization-defined time-period*] of the release of the updates; and

(f) Incorporate flaw remediation of personally identifiable information into the organizational configuration management process.

Supplemental Guidance: None.

Related Controls: IR-4, IR-5, PM-23.

References: FIPS Publications 140-2, 186-4; NIST Special Publications 800-40, 800-128; NIST Interagency Report 7788.

SI-3 MALICIOUS CODE PROTECTION

Control:

a. ~~Employs~~Implement [*Selection (one or more): signature based; non-signature based*] malicious code protection mechanisms at ~~information~~ system entry and exit points to detect and eradicate malicious code;

b. Automatically update malicious code protection mechanisms whenever 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/exit points*] as the files are downloaded, opened, or executed in accordance with organizational ~~security~~ policy; and

2. [*Selection (one or more): block malicious code; quarantine malicious code; send alert to administrator;* [*Assignment: organization-defined action*]] 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.

Supplemental Guidance: System entry and exit points include, for example, firewalls, remote-access servers, workstations, electronic mail servers, web servers, proxy servers, ~~remote-access servers, workstations,~~ notebook computers, and mobile devices. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats ~~(e.g., UUENCODE, Unicode),~~ contained within compressed or hidden files, or hidden in files using techniques such as steganography. Malicious code can be ~~transported by different means~~inserted into systems in a variety of ways including, for example, ~~web accesses,~~ by electronic mail, ~~electronic mail attachments~~the world-wide web, and portable storage devices. Malicious code insertions occur through the exploitation of ~~information~~ system vulnerabilities. ~~Malicious code protection mechanisms include, for example, anti-virus signature definitions and reputation-based technologies.~~ A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Malicious code protection mechanisms include, for example, signature- and nonsignature-based technologies. Nonsignature-based detection mechanisms include, for example, artificial intelligence techniques that use heuristics to detect, analyze, and describe the characteristics or behavior of malicious code and to provide safeguards against such code for which signatures do not yet exist or for which existing signatures may not be effective. This 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 execution of unauthorized code. ~~In addition to~~ Malicious code may be present in commercial off-the-shelf software~~, malicious code may also be present~~ and in custom-built software. This could include, for example, logic bombs, back doors, and other types of ~~cyber~~ attacks that could affect organizational missions and business functions.

In situations where malicious code ~~protection mechanisms~~ cannot ~~always detect such code. In these situations~~be detected by detection methods and technologies, organizations rely instead on other types of safeguards including, for example, secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended. Organizations may determine that in response to the detection of malicious code, different actions may be warranted. For example, organizations can define actions in response to malicious code detection during periodic scans, actions in response to detection of malicious downloads, or actions in response to detection of maliciousness when attempting to open or execute files. Due to system integrity and availability concerns, organizations consider the specific methodology used to carry out automatic updates.

Related Controls: AC-4, AC-19, CM-3, CM-8, IR-4, MA-3, MA-4, RA-5, SC-7, SC-26, SC-28, SC-23, SC-44, SI-2, SI-4, SI-7, SI-8, SI-15.

Control Enhancements:

(1) MALICIOUS CODE PROTECTION | CENTRAL MANAGEMENT

Centrally manage malicious code protection mechanisms.

Supplemental Guidance: Central management is the organization-wide management and implementation of malicious code protection mechanisms. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed flaw and malicious code protection ~~security~~ controls.

Related Controls: PL-9.

(2) MALICIOUS CODE PROTECTION | AUTOMATIC UPDATES

~~**The information system automatically updates malicious code protection mechanisms.**~~

Supplemental Guidance: Malicious code protection mechanisms include, for example, signature definitions. Due to information system integrity and availability concerns, organizations give careful consideration to the methodology used to carry out automatic updates. Related control: SI-8.

[Withdrawn: Incorporated into SI-3].

(3) MALICIOUS CODE PROTECTION | NON-PRIVILEGED USERS

[Withdrawn: Incorporated into AC-6 (10)].

(4) MALICIOUS CODE PROTECTION | UPDATES ONLY BY PRIVILEGED USERS

Update malicious code protection mechanisms only when directed by a privileged user.

Supplemental Guidance: This control enhancement may be appropriate for is employed in situations where for reasons of security or operational continuity, updates to malicious code protection mechanisms are only applied when selected/approved by designated organizational personnel.

Related Controls: CM-5.

(5) MALICIOUS CODE PROTECTION | PORTABLE STORAGE DEVICES

[Withdrawn: Incorporated into MP-7].

(6) MALICIOUS CODE PROTECTION | TESTING AND VERIFICATION

(a) Test malicious code protection mechanisms [*Assignment: organization-defined frequency*] by introducing a known benign, non-spreading test case into the system; and

(b) Verify that the detection of the test case and the associated incident reporting occur.

Supplemental Guidance: None.

Related Controls: CA-2, CA-7, RA-5.

(7) MALICIOUS CODE PROTECTION | NONSIGNATURE-BASED DETECTION

The information system implements nonsignature-based malicious code detection mechanisms.

Supplemental Guidance: Nonsignature-based detection mechanisms include, for example, the use of heuristics to detect, analyze, and describe the characteristics or behavior of malicious code and to provide safeguards against malicious code for which signatures do not yet exist or for which existing signatures may not be effective. [Withdrawn: Incorporated into SI-3].

(8) This includes polymorphic malicious code (i.e., code that changes signatures when it replicates). This control enhancement does not preclude the use of signature-based detection mechanisms.

(9)(8) MALICIOUS CODE PROTECTION | DETECT UNAUTHORIZED COMMANDS

Detect [*Assignment: organization-defined unauthorized operating system commands*] through the kernel application programming interface at [*Assignment: organization-defined system hardware components*] and [*Selection (one or more): issue a warning; audit the command execution; prevent the execution of the command*].

Supplemental Guidance: This control enhancement can also be applied to critical interfaces other than kernel-based interfaces, including for example, interfaces with virtual machines and privileged applications. Unauthorized operating system commands include, for example, commands for kernel functions from system processes that are not trusted to initiate such commands, or commands for kernel functions that are suspicious even though commands of that type are reasonable for processes to initiate. Organizations can define the malicious commands to be detected by a combination of command types, command classes, or specific instances of commands. Organizations can define hardware components by specific component type, component type, component location in the network, or combination therein. Organizations may select different actions for different types/, classes/specific, or instances of potentially malicious commands.

Related Controls: AU-2, AU-6, AU-12.

(10)(9) MALICIOUS CODE PROTECTION | AUTHENTICATE REMOTE COMMANDS

Implement [*Assignment: organization-defined security safeguards*] to authenticate [*Assignment: organization-defined remote commands*].

Supplemental Guidance: This control enhancement protects against unauthorized commands and replay of authorized commands. This capability is important for those remote systems whose loss, malfunction, misdirection, or exploitation would have immediate and/or serious consequences ~~(e.g.,~~ , including, for example, injury or death, property damage, loss of high-~~valued~~value assets, compromise of classified or ~~sensitive~~controlled unclassified information, or failure of ~~important~~ missions or business functions. Authentication safeguards for remote commands ~~help to~~ ensure that ~~information~~ systems accept and execute commands in the order intended, execute only authorized commands, and ~~that~~reject unauthorized commands ~~are rejected.~~ Cryptographic mechanisms can be employed, for example, to authenticate remote commands.

Related Controls: SC-12, SC-13, SC-23.

~~(11)~~**(10)** MALICIOUS CODE PROTECTION | MALICIOUS CODE ANALYSIS

(a) Employ [*Assignment: organization-defined tools and techniques*] to analyze the characteristics and behavior of malicious code; and

(b) Incorporate the results from malicious code analysis into organizational incident response and flaw remediation processes.

Supplemental Guidance: The ~~application~~use of ~~selected~~ malicious code analysis tools ~~and techniques~~ 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 more effective organizational responses to current and future threats. Organizations can also conduct malicious code analyses by using reverse engineering techniques or by monitoring the behavior of executing code.

Related Controls: None.

References: NIST Special Publication 800-83, 800-125B, 800-177.

SI-4 SYSTEM MONITORING

Control:

a. Monitor the system to detect:

   1. Attacks and indicators of potential attacks in accordance with [*Assignment: organization-defined monitoring objectives*]; and

   2. Unauthorized local, network, and remote connections;

b. Identify unauthorized use of the system through [*Assignment: organization-defined techniques and methods*];

c. ~~Deploys~~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. Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;

e. ~~Heightens~~Adjust the level of system monitoring activity when there is ~~an indication of increased~~a change in risk to organizational operations and assets, individuals, other organizations, or the Nation ~~based on law enforcement information, intelligence information, or other credible sources of information~~;

f. Obtain legal opinion regarding system monitoring activities ~~in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations~~; 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*]].

Supplemental Guidance: System monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at system ~~boundary (i.e., part of perimeter defense and boundary protection).~~boundaries. Internal monitoring includes the observation of events occurring within the ~~information~~ system. Organizations monitor systems, for example, by observing audit activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions. The monitoring objectives ~~may~~ guide and inform the determination of the events. System monitoring capability is achieved through a variety of tools and techniques, including, for example, intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, ~~network monitoring software).~~and network monitoring software. The distribution and configuration of monitoring devices can impact throughput at key internal and external boundaries, and at other locations across a network due to the introduction of network throughput latency. Therefore, such devices are strategically located and deployed as part of an established organization-wide security architecture. Strategic locations for monitoring devices include, for example, selected perimeter locations and near key servers and server farms supporting critical applications. Monitoring devices are typically employed at the managed interfaces associated with controls SC-7 and AC-17. ~~Einstein network monitoring devices from the Department of Homeland Security can also be included as monitoring devices. The granularity of monitoring~~The information collected is ~~based on~~a function of the organizational monitoring objectives and the capability of systems to support such objectives. Specific types of transactions of interest include, for example, Hyper Text Transfer Protocol (HTTP) traffic that bypasses HTTP proxies. System monitoring is an integral part of organizational continuous monitoring and incident response programs~~. Output from system monitoring serves as input to continuous monitoring and incident response programs. A network connection is any connection with a device that communicates through a network (e.g., local area network, Internet). A remote connection is any connection with a device communicating through an external network (e.g., the Internet). Local, network, and remote connections can be either wired or wireless. Related controls: AC-3, AC-4, AC-8, AC-17, AU-2, AU-6, AU-7, AU-9, AU-12, CA-7, IR-4, PE-3, RA-5, SC-7, SC-26, SC-35, SI-3, SI-7~~ and output from system monitoring serves as input to those programs. Adjustments to levels of system monitoring are based on law enforcement information, intelligence information, or other credible sources of information. The legality of system monitoring activities is based on applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines.

Related Controls: AC-2, AC-3, AC-4, AC-8, AC-17, AU-2, AU-6, AU-7, AU-9, AU-12, AU-14, CA-7, CM-3, CM-8, CM-11, IA-10, IR-4, PE-3, PM-12, PM-24, RA-5, SA-18, SC-7, SC-26, SC-31, SC-35, SC-36, SC-37, SI-3, SI-6, SI-7.

Control Enhancements:

(1) SYSTEM MONITORING | SYSTEM-WIDE INTRUSION DETECTION SYSTEM

Connect and configure individual intrusion detection tools into a system-wide intrusion detection system.

Supplemental Guidance: CM-6.

Related Controls: None.

(2) SYSTEM MONITORING | AUTOMATED TOOLS AND MECHANISMS FOR REAL-TIME ANALYSIS

Employ automated tools and mechanisms to support near real-time analysis of events.

Supplemental Guidance: Automated tools and mechanisms include, for example, host-based, network-based, transport-based, or storage-based event monitoring tools and mechanisms or Security Information and Event Management technologies that provide real time analysis of alerts and notifications generated by organizational systems.

Related Controls: None.

(3) SYSTEM MONITORING | AUTOMATED TOOL AND MECHANISM INTEGRATION

Employ automated tools and mechanisms to integrate intrusion detection tools and mechanisms into access control and flow control mechanisms ~~for~~.

Supplemental Guidance: Using automated tools and mechanisms to integrate intrusion detection tools and mechanisms into access and flow control mechanisms facilitates a rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination.

~~*INFORMATION*~~ Related Controls: None.

(4) SYSTEM MONITORING | INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC

Monitor inbound and outbound communications traffic [*Assignment: organization-defined frequency*] for unusual or unauthorized activities or conditions.

Supplemental Guidance: Unusual or unauthorized activities or conditions related to system inbound and outbound communications traffic include, for example, internal traffic that indicates the presence of malicious code within organizational systems or propagating among system components; the unauthorized exporting of information; or signaling to external systems. Evidence of malicious code is used to identify potentially compromised systems or system components.

Related Controls: None.

(5) SYSTEM MONITORING | SYSTEM-GENERATED ALERTS

Alert [*Assignment: organization-defined personnel or roles*] when the following system-generated indications of compromise or potential compromise occur: [*Assignment: organization-defined compromise indicators*].

Supplemental Guidance: Alerts may be generated from a variety of sources, including, for example, audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers. Alerts can be automated or they may be transmitted, for example, telephonically, by electronic mail messages, or by text messaging. Organizational personnel on the alert notification list can include, for example, system administrators, mission or business owners, system owners, system security officers, or privacy officers. This control enhancement focuses on the security alerts generated by the system. Alternatively, alerts generated by organizations in SI-4(12) focus on information sources external to the system such as suspicious activity reports and reports on potential insider threats.

Related Controls: AU-4, AU-5, PE-6.

(6) SYSTEM MONITORING | RESTRICT NON-PRIVILEGED USERS

[Withdrawn: Incorporated into AC-6(10)].

(7) SYSTEM MONITORING | AUTOMATED RESPONSE TO SUSPICIOUS EVENTS

Notify [*Assignment: organization-defined incident response personnel (identified by name and/or by role)*] of detected suspicious events and take [*Assignment: organization-defined least-disruptive actions to terminate suspicious events*].

Supplemental Guidance: Least-disruptive actions include, for example, initiating requests for human responses.

Related Controls: None.

(8) SYSTEM MONITORING | PROTECTION OF MONITORING INFORMATION

[Withdrawn: Incorporated into SI-4].

(9) SYSTEM MONITORING | TESTING OF MONITORING TOOLS AND MECHANISMS

Test intrusion-monitoring tools and mechanisms [*Assignment: organization-defined frequency*].

Supplemental Guidance: Testing intrusion-monitoring tools and mechanism is necessary to ensure that the tools and mechanisms are operating correctly and continue to ~~meet~~satisfy the monitoring objectives of organizations. The frequency of testing depends on the types of tools and mechanisms used by organizations and the methods of deployment.

Related Controls: CP-9.

(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*].

Supplemental Guidance: Organizations balance the potentially conflicting needs for encrypting communications traffic and having visibility into such traffic from a monitoring perspective. For some organizations, the need to ensure the confidentiality of communications traffic is paramount; for ~~others~~other organizations, mission assurance is of greater concern. Organizations determine whether the visibility requirement applies to internal encrypted traffic, encrypted traffic intended for external destinations, or a subset of the traffic types.

Related Controls: None.

(11) SYSTEM MONITORING | ANALYZE COMMUNICATIONS TRAFFIC ANOMALIES

Analyze outbound communications traffic at the external boundary of the system and selected [*Assignment: organization-defined interior points within the system ~~(e.g., subnetworks, subsystems)~~*]] to discover anomalies.

Supplemental Guidance: Examples of organization-defined interior points within the system include subnetworks and subsystems. Anomalies within organizational systems include, for example, large file transfers; long-time persistent connections; unusual protocols and ports in use; and attempted communications with suspected malicious external addresses.

Related Controls: None.

(12) SYSTEM MONITORING | AUTOMATED ~~*ALERTS*~~ ORGANIZATIONGENERATED ALERTS

Employ automated mechanisms to alert ~~security~~ [*Assignment: organization-defined personnel or roles*] when the following organization-generated indications of inappropriate or unusual activities with security or privacy implications occur: [*Assignment: organization-defined activities that trigger alerts*].

Supplemental Guidance: Organizational personnel on the alert notification list can include, for example, system administrators, mission or business owners, system owners, system security officers, or privacy officers. This control enhancement focuses on the security alerts generated by organizations and transmitted using automated means. In contrast to the alerts generated by ~~information~~ systems in SI-4(5) that focus on information sources that are internal to the systems such as audit records, the sources of information for this enhancement focus on other entities such as suspicious activity reports and reports on potential insider threats.

Related Controls: None.

~~(12)~~(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/or events~~; and

(c) Use the traffic and event profiles in tuning system-monitoring devices to reduce the number of false positives and false negatives.

Supplemental Guidance: None.

Related Controls: None.

~~(13)~~(14) SYSTEM MONITORING | WIRELESS INTRUSION DETECTION

Employ a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises or breaches to the system.

Supplemental Guidance: Wireless signals may radiate beyond organization-controlled facilities. Organizations proactively search for unauthorized wireless connections including the conduct of thorough scans for unauthorized wireless access points. Scans are not limited to those areas within facilities containing systems, but also include areas outside of facilities to verify that unauthorized wireless access points are not connected to organizational systems.

Related Controls: AC-18, IA-3.

~~(14)~~(15) SYSTEM MONITORING | WIRELESS TO WIRELINE COMMUNICATIONS

Employ an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wireline networks.

Supplemental Guidance: None.

Related Controls: AC-18.

~~(15)~~(16) SYSTEM MONITORING | CORRELATE MONITORING INFORMATION

Correlate information from monitoring tools and mechanisms employed throughout the system.

Supplemental Guidance: Correlating information from different system monitoring tools and mechanisms can provide a more comprehensive view of ~~information~~ system activity. Correlating system monitoring tools and mechanisms that ~~usually~~typically work in isolation ~~(e.g.,~~including, for example, anti-virus software, host monitoring, and network monitoring, ~~anti-virus software)~~ can provide an organization-wide monitoring view and may reveal otherwise unseen attack patterns. Understanding capabilities and limitations of diverse monitoring tools and mechanisms and how to maximize the utility of information generated by those tools and mechanisms can help organizations to ~~build~~develop, operate, and maintain effective monitoring programs.

Related Controls: AU-6.

~~(16)~~(17) SYSTEM MONITORING | INTEGRATED SITUATIONAL AWARENESS

Correlate information from monitoring physical, cyber, and supply chain activities to achieve integrated, organization-wide situational awareness.

Supplemental Guidance: This control enhancement correlates monitoring information from a more diverse set of information sources to achieve integrated situational awareness. Integrated situational awareness from a combination of physical, cyber, and supply chain monitoring activities enhances the capability of organizations to more quickly detect sophisticated attacks and investigate the methods and techniques employed to carry out such attacks. In contrast to SI-4(16) which correlates the various cyber monitoring information, this control enhancement correlates monitoring beyond the cyber domain. Such monitoring may help reveal attacks on organizations that are operating across multiple attack vectors.

Related Controls: AU-16, PE-6, SA-12.

~~(17)~~(18) SYSTEM MONITORING | ANALYZE TRAFFIC AND COVERT EXFILTRATION

Analyze outbound communications traffic at the external boundary or perimeter of the system and at [*Assignment: organization-defined interior points within the system~~(e.g., subsystems, subnetworks)~~*]] to detect covert exfiltration of information.

Supplemental Guidance: Examples of organization-defined interior points within the system include subnetworks and subsystems. Covert means that can be used for the ~~unauthorized~~ exfiltration of ~~organizational~~ information include, for example, steganography.

Related Controls: None.

~~(18)~~(19) SYSTEM MONITORING | INDIVIDUALS POSING GREATER RISK

Implement [*Assignment: organization-defined additional monitoring*] of individuals who have been identified by [*Assignment: organization-defined sources*] as posing an increased level of risk.

Supplemental Guidance: Indications of increased risk from individuals can be obtained from a variety of sources including, for example, human resource records, intelligence agencies, law enforcement organizations, and other credible sources. The monitoring of specific individuals is closely coordinated with management, legal, security, privacy and human ~~resources~~resource officials within organizations conducting such monitoring ~~and complies~~. Monitoring is conducted in accordance with ~~federal legislation~~applicable laws, Executive Orders, ~~policies,~~ directives, regulations, policies, standards, and guidelines.

Related Controls: None.

~~(19)~~(20) SYSTEM MONITORING | PRIVILEGED USERS

Implement [*Assignment: organization-defined additional monitoring*] of privileged users.

Supplemental Guidance: None.

Related Controls: AC-18.

~~(20)~~(21) SYSTEM MONITORING | PROBATIONARY PERIODS

Implement [*Assignment: organization-defined additional monitoring*] of individuals during [*Assignment: organization-defined probationary period*].

Supplemental Guidance: None.

Related Controls: AC-18.

~~(21)~~(22) SYSTEM MONITORING | UNAUTHORIZED NETWORK SERVICES

Detect network services that have not been authorized or approved by [*Assignment: organization-defined authorization or approval processes*] and [*Selection (one or more): audit; alert* [*Assignment: organization-defined personnel or roles*]].

Supplemental Guidance: Unauthorized or unapproved network services include, for example, services in service-oriented architectures that lack organizational verification or validation and therefore may be unreliable or serve as malicious rogues for valid services.

Related Controls: CM-7.

~~(22)~~(23) SYSTEM MONITORING | HOST-BASED DEVICES

Implement [*Assignment: organization-defined host-based monitoring mechanisms*] at [*Assignment: organization-defined system components*].

Supplemental Guidance: System components where host-based monitoring can be implemented include, for example, servers, ~~workstations~~notebook computers, and mobile devices. Organizations may consider employing host-based monitoring mechanisms from multiple ~~information technology~~ product developers or vendors.

Related Controls: AC-18, AC-19.

~~(23)~~(24) SYSTEM MONITORING | INDICATORS OF COMPROMISE

Discover, collect, and distribute to [*Assignment: organization-defined personnel or roles*], indicators of compromise.

Supplemental Guidance: Indicators of compromise (IOC) are forensic artifacts from intrusions that are identified on organizational systems at the host or network level. IOCs provide ~~organizations with~~ valuable information on ~~objects or information~~ systems that have been compromised. IOCs for the discovery of compromised hosts can include, for example, the creation of registry key values. IOCs for network traffic include, for example, Universal Resource Locator or protocol elements that indicate ~~malware~~malicious code command and control servers. The rapid distribution and adoption of IOCs can improve information security by reducing the time that systems and organizations are vulnerable to the same exploit or attack.Related Controls: AC-18.

(25) SYSTEM MONITORING | PERSONALLY IDENTIFIABLE INFORMATION MONITORING

Employ automated mechanisms to monitor:

(a) For unauthorized access or usage of personally identifiable information; and

(b) The collection, creation, accuracy, relevance, timeliness, impact, and completeness of personally identifiable information.

Supplemental Guidance: Monitoring the collection, creation, accuracy, relevance, timeliness, impact, and completeness of personally identifiable information helps improve data quality. Automated monitoring techniques can create unintended privacy risks because automated controls may connect to external or otherwise unrelated systems. The matching of records between these systems may create linkages with unintended consequences. Organizations assess and document these risks in their privacy impact assessment and make determinations that are in alignment with their privacy program plan.

Related Controls: PM-24, PM-26, SI-19.

References: NIST Special Publications 800-61, 800-83, 800-92, 800-94, 800-137.

SI-5 SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

Control:

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.

Supplemental Guidance: The United States Computer Emergency Readiness Team (US-CERT) generates security alerts and advisories to maintain situational awareness across the federal government. Security directives are issued by OMB or other designated organizations with the responsibility and authority to issue such directives. Compliance to security directives is essential due to the critical nature of many of these directives and the potential immediate adverse effects on organizational operations and assets, individuals, other organizations, and the Nation should the directives not be implemented in a timely manner. External organizations include, for example, external mission or business partners, supply chain partners, external service providers, and other peer or supporting organizations.

Related Controls: PM-15, RA-5, SI-2.

Control Enhancements:

(1) SECURITY ALERTS, ADVISORIES, AND DIRECTIVES | AUTOMATED ALERTS AND ADVISORIES

Employ automated mechanisms to make security alert and advisory information available throughout the organization.

Supplemental Guidance: The significant number of changes to organizational systems and the environments in which those systems operate requires the dissemination of security-related information to a variety of organizational entities that have a direct interest in the success of organizational missions and business functions. Based on information provided by security alerts and advisories, changes may be required at one or more of the three tiers related to the management of information security and privacy risk including the governance level, mission and business process~~/enterprise architecture~~ level, and the system level.

Related Controls: None.

References: NIST Special Publication 800-40.

SI-6 SECURITY AND PRIVACY FUNCTION VERIFICATION

Control:

a. Verify the correct operation of [*Assignment: organization-defined security and privacy functions*];

b. Perform this verification [*Selection (one or more):* [*Assignment: organization-defined system transitional states*]*; upon command by user with appropriate privilege;* [*Assignment: organization-defined frequency*]];

c. Notify [*Assignment: organization-defined personnel or roles*] of 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.

Supplemental Guidance: Transitional states for systems include, for example, system startup, restart, shutdown, and abort. Notifications by the system include, for example, hardware indicator lights, electronic alerts to system administrators, and messages to local computer consoles~~, and/or hardware indications such~~. In contrast to security function verification, privacy function verification ensures that privacy functions operate as ~~lights.~~ expected and are approved by the Senior Agency Official for Privacy, or that privacy attributes are applied or used as expected.

Related Controls: CA-7, CM-4, CM-6, SI-7.

Control Enhancements:

(1) SECURITY AND PRIVACY FUNCTION VERIFICATION | NOTIFICATION OF FAILED SECURITY TESTS

[Withdrawn: Incorporated into SI-6].

(2) SECURITY AND PRIVACY FUNCTION VERIFICATION | AUTOMATION SUPPORT FOR DISTRIBUTED TESTING

Implement automated mechanisms to support the management of distributed security and privacy function testing.

Supplemental Guidance: None.

Related Controls: SI-2.

(3) SECURITY AND PRIVACY FUNCTION VERIFICATION | REPORT VERIFICATION RESULTS

Report the results of security and privacy function verification to [*Assignment: organization-defined personnel or roles*].

Supplemental Guidance: Organizational personnel with potential interest in the results of the verification of security and privacy function include, for example, ~~senior information security officers~~ system security managers, systems security officers, Senior Agency Information Security Officers, and Senior Agency Officials for Privacy.

Related Controls: SA-12, SI-4.

References: None.

SI-7 SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY

Control: Employ integrity verification tools to detect unauthorized changes to [*Assignment: organization-defined software, firmware, and information*].

Supplemental Guidance: Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity ~~(e.g., tampering).~~ Software includes, for example, operating systems (with key internal components such as kernels, drivers), middleware, and applications. Firmware includes, for example, the Basic Input Output System (BIOS). Information includes personally identifiable information and metadata containing security and privacy attributes associated with information. Integrity-checking mechanisms including, for example, parity checks, cyclical redundancy checks, cryptographic hashes, and associated tools can automatically monitor the integrity of systems and hosted applications.

Related Controls: AC-4, CM-3, CM-7, CM-8, MA-3, MA-4, RA-5, SA-9, SA-10, SA-18, SA-19, CM-7, SA-12, SC-8, SC-13, SC-28, SC-37, SI-3.

Control Enhancements:

(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*]].

Supplemental Guidance: Security-relevant events include, for example, the identification of a new threat to which organizational systems are susceptible, and the installation of new hardware, software, or firmware. Transitional states include, for example, system startup, restart, shutdown, and abort.

Related Controls: None.

(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.

Supplemental Guidance: The use of automated tools to report integrity violations and to notify organizational personnel in a timely matter is an essential precursor to effective risk response. Personnel having an interest in integrity violations include, for example, mission and business owners, system owners, systems administrators, software developers, systems integrators, and information security officers, and privacy officers.

Related Controls: None.

(3) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CENTRALLY-MANAGED INTEGRITY TOOLS

Employ centrally managed integrity verification tools.

Supplemental Guidance: None.

Related Controls: AU-3, SI-2, SI-8.

(4) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | TAMPER-EVIDENT PACKAGING

[Withdrawn: Incorporated into SA-12].

(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 security safeguards*]] when integrity violations are discovered.

Supplemental Guidance: Organizations may define different integrity checking responses by type of information, by specific information, or a combination of both. Examples of types of information include firmware, software, and user data. Examples of specific information include boot firmware for certain types of machines~~; or a combination of both.~~ . The automatic implementation of ~~specific~~ safeguards within organizational systems includes, for example, reversing the changes, halting the system, or triggering audit alerts when unauthorized modifications to critical security files occur.

Related Controls: None.

(6) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CRYPTOGRAPHIC PROTECTION

Implement cryptographic mechanisms to detect unauthorized changes to software, firmware, and information.

Supplemental Guidance: Cryptographic mechanisms used for the protection of integrity include, for example, digital signatures and the computation and application of signed hashes using asymmetric cryptography; protecting the confidentiality of the key used to generate the hash; and using the public key to verify the hash information.

Related Controls: SC-12, SC-13.

(7) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRATION OF DETECTION AND RESPONSE

Incorporate the detection of the following unauthorized changes into the organizational incident response capability: [*Assignment: organization-defined security-relevant changes to the system*].

Supplemental Guidance: This control enhancement helps to ensure that detected events are tracked, monitored, corrected, and available for historical purposes. Maintaining historical records is important both for being able to identify and discern adversary actions over an extended time-period and for possible legal actions. Security-relevant changes include, for example, unauthorized changes to established configuration settings or unauthorized elevation of system privileges.

Related Controls: AU-2, AU-6, IR-4, IR-5, SI-4.

(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 initiate the following actions: [*Selection (one or more): generate an audit record; alert current user; alert* [*Assignment: organization-defined personnel or roles*]; [*Assignment: organization-defined other actions*]].

Supplemental Guidance: Organizations select response actions based on types of software, specific software, or information for which there are potential integrity violations.

Related Controls: AU-2, AU-6, AU-12.

(9) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | VERIFY BOOT PROCESS

Verify the integrity of the boot process of [*Assignment: organization-defined* ~~*devices*~~*system components*].

Supplemental Guidance: Ensuring the integrity of boot processes is critical to starting ~~devices~~system components in known, trustworthy states. Integrity verification mechanisms provide ~~organizational personnel with~~a level of assurance that only trusted code is executed during boot processes.

Related Controls: SI-6.

(10) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | PROTECTION OF BOOT FIRMWARE

Implement [*Assignment: organization-defined security safeguards*] to protect the integrity of boot firmware in [*Assignment: organization-defined ~~devices~~system components*].

Supplemental Guidance: Unauthorized modifications to boot firmware may be indicative of a sophisticated, targeted ~~cyber~~ attack. These types of ~~cyber~~targeted attacks can result in a permanent denial of service ~~(e.g., if the firmware is corrupted)~~ or a persistent malicious code presence ~~(e.g.,~~. These situations can occur, for example, if the firmware is corrupted or if the malicious code is embedded within the firmware~~). Devices~~. System components can protect the integrity of boot firmware in organizational systems by verifying the integrity and authenticity of all updates to the firmware prior to applying changes to the ~~boot devices~~system component; and preventing unauthorized processes from modifying the boot firmware.

Related Controls: SI-6.

(11) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CONFINED ENVIRONMENTS WITH LIMITED PRIVILEGES

Require that [*Assignment: organization-defined user-installed software*] execute in a confined physical or virtual machine environment with limited privileges.

Supplemental Guidance: Organizations identify software that may be of concern regarding its origin or potential for containing malicious code. For this type of software, user installations occur in confined environments of operation to limit or contain damage from malicious code that may be executed.

Related Controls: CM-11, SC-44.

(12) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRITY VERIFICATION

Require that the integrity of [*Assignment: organization-defined user-installed software*] be verified prior to execution.

Supplemental Guidance: Organizations verify the integrity of user-installed software prior to execution to reduce the likelihood of executing malicious code or code that contains errors from unauthorized modifications. Organizations consider the practicality of approaches to verifying software integrity including, for example, availability of checksums of adequate trustworthiness from software developers or vendors.

Related Controls: CM-11.

(13) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CODE EXECUTION IN PROTECTED ENVIRONMENTS

Allow execution of binary or machine-executable ~~code obtained from sources with limited or no warranty and without the provision of source~~ 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.

Supplemental Guidance: This control enhancement applies to all sources of binary or machine-executable code including, for example, commercial software and firmware and open source software.

Related Controls: CM-10, SC-44.

(14) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | BINARY OR MACHINE EXECUTABLE CODE

(a) Prohibit the use of binary or machine-executable code from sources with limited or no warranty and without the provision of source code; and

(b) Provide exceptions to the source code requirement only for compelling mission or operational requirements and with the approval of the authorizing official.

Supplemental Guidance: This control enhancement applies to all sources of binary or machine-executable code including, for example, commercial software and firmware and open source software. Organizations assess software products without accompanying source code from sources with limited or no warranty for potential security impacts. The assessments address the fact that these types of software products may be difficult to review, repair, or extend,

given that organizations, in most cases, do not have access to the original source code. In addition, there may be no owners who could make such repairs on behalf of organizations.

Related Controls: SA-5.

(15) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CODE AUTHENTICATION

Implement cryptographic mechanisms to authenticate [*Assignment: organization-defined software or firmware components*] prior to installation.

Supplemental Guidance: Cryptographic authentication includes, for example, verifying that software or firmware components have been digitally signed using certificates recognized and approved by organizations. Code signing is an effective method to protect against malicious code.

Related Controls: CM-5.

(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*].

Supplemental Guidance: This control enhancement addresses processes for which typical or normal execution periods can be determined and situations in which organizations exceed such periods. Supervision includes, for example, timers on operating systems, automated responses, or manual oversight and response when system process anomalies occur.

Related Controls: None.

References: FIPS Publications 140-2, 180-4, 186-4, 202; NIST Special Publications 800-70, 800-147.

SI-8 SPAM PROTECTION

Control:

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.

Supplemental Guidance: System entry and exit points include, for example, firewalls, remote-access servers, electronic mail servers, web servers, proxy servers, workstations, notebook~~/laptop~~ computers, and mobile devices. Spam can be transported by different means including, for example, electronic mail, electronic mail attachments, and web accesses. Spam protection mechanisms include, for example, signature definitions.

Related Controls: SC-5, SC-7, SC-38, SI-3, SI-4.

Control Enhancements:

(1) SPAM PROTECTION | CENTRAL MANAGEMENT

Centrally manage spam protection mechanisms.

Supplemental Guidance: Central management is the organization-wide management and implementation of spam protection mechanisms. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed spam protection controls.

Related Controls: AU-3, CM-6, SI-2, SI-7.

(2) SPAM PROTECTION | AUTOMATIC UPDATES

Automatically update spam protection mechanisms.

Supplemental Guidance: None.

Related Controls: None.

(3) SPAM PROTECTION | CONTINUOUS LEARNING CAPABILITY

Implement spam protection mechanisms with a learning capability to more effectively identify legitimate communications traffic.

Supplemental Guidance: Learning mechanisms include, for example, Bayesian filters that respond to user inputs identifying specific traffic as spam or legitimate by updating algorithm parameters and thereby more accurately separating types of traffic.

Related Controls: None.

References: NIST Special Publications 800-45, 800-177.

SI-9 INFORMATION INPUT RESTRICTIONS

[Withdrawn: Incorporated into AC-2, AC-3, AC-5, AC-6].

SI-10 INFORMATION INPUT VALIDATION

Control: Check the validity of [*Assignment: organization-defined information inputs*].

Supplemental Guidance: Checking the valid syntax and semantics of system inputs including, for example, character set, length, numerical range, and acceptable values, verifies that inputs match specified definitions for format and content. Software 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 to interpreters prevents the content from being unintentionally interpreted as commands. Input validation ensures accurate and correct inputs and prevent attacks such as cross-site scripting and a variety of injection attacks.

Related Controls: None.

Control Enhancements:

(1) INFORMATION INPUT VALIDATION | MANUAL OVERRIDE CAPABILITY

(a) Provide a manual override capability for input validation of [*Assignment: organization-defined inputs*];

(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.

Supplemental Guidance: In certain situations, for example, during events that are defined in organizational contingency plans, a manual override capability for input validation may be needed. Such manual overrides are used only in limited circumstances and with the inputs defined by the organization.

Related Controls: AC-3, AU-2, AU-12.

(2) INFORMATION INPUT VALIDATION | REVIEW ~~/ *RESOLUTION OF*~~AND RESOLVE ERRORS

Review and resolve input validation errors within [*Assignment: organization-defined time-period*].

Supplemental Guidance: Resolution of input validation errors includes, for example, correcting systemic causes of errors and resubmitting transactions with corrected input.

Related Controls: None.

(3) INFORMATION INPUT VALIDATION | PREDICTABLE BEHAVIOR

Verify that the system behaves in a predictable and documented manner ~~that reflects organizational and system objectives~~ when invalid inputs are received.

Supplemental Guidance: A common vulnerability in organizational systems is unpredictable behavior when invalid inputs are received. This control enhancement ensures that there is predictable behavior in the face of invalid inputs by specifying system responses that facilitate

transitioning the system to known states without adverse, unintended side effects. The invalid inputs are those inputs related to the information inputs defined by the organization in the base control.

Related Controls: None.

(4) INFORMATION INPUT VALIDATION | ~~*REVIEW /*~~ TIMING INTERACTIONS

Account for timing interactions among system components in determining appropriate responses for invalid inputs.

Supplemental Guidance: In addressing invalid system inputs received across protocol interfaces, timing ~~interfaces~~interactions become relevant, where one protocol needs to consider the impact of the error response on other protocols within 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 collisions or noise on the link. If TCP makes a congestion response, it takes ~~precisely~~ the wrong action in response to a collision event. Adversaries may be able to use ~~apparently~~what appears to be acceptable individual behaviors of the protocols in concert to achieve adverse effects through suitable construction of invalid input.

Related Controls: None.

(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/or [*Assignment: organization-defined formats*].

Supplemental Guidance: This control enhancement applies the concept of whitelisting to information inputs. Specifying known trusted sources for information inputs and acceptable formats for such inputs can reduce the probability of malicious activity.

Related Controls: AC-3, AC-6.

References: NIST Special Publication 800-167.

SI-11 ERROR HANDLING

Control:

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*].

Supplemental Guidance: Organizations consider the structure and the content of error messages. The extent to which systems can handle error conditions is guided and informed by organizational policy and operational requirements. Exploitable information includes, for example, erroneous logon attempts with passwords entered by mistake as the username; mission/business information that can be derived from, if not stated explicitly by, the information recorded; and ~~personal~~personally identifiable information such as account numbers, social security numbers, and credit card numbers. In addition, error messages may provide a covert channel for transmitting information.

Related Controls: AU-2, AU-3, SC-31, SI-2.

Control Enhancements: None.

References: None.

SI-12 INFORMATION ~~HANDLING~~MANAGEMENT AND RETENTION

Control: ~~handles~~Manage and retain information within the system and information output from the system in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, guidelines and operational requirements.

Supplemental Guidance: Information ~~handling~~management and retention requirements cover the full life cycle of information, in some cases extending beyond system disposal. Information to be retained may also include policies, procedures, plans, and other types of administrative information. The National Archives and Records Administration provides guidance on records retention.

Related Controls: All XX-1 Controls, 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, PA-1, PA-2, PA-3, PL-2, PL-4, PM-4, PM-8, PM-9, PS-2, PS-6, RA-2, RA-3, SA-5.

Control Enhancements:

(1) INFORMATION MANAGEMENT AND RETENTION | LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS

Limit personally identifiable information being processed in the information life cycle to the [*Assignment: organization-defined elements*] identified in the privacy risk assessment.

Supplemental Guidance: Limiting the use of personally identifiable information throughout the information life cycle when such information is not needed for operational purposes helps reduce the level of privacy risk created by a system. The information life cycle includes information creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposition.

Related Controls: None.

(2) INFORMATION MANAGEMENT AND RETENTION | MINIMIZE PERSONALLY IDENTIFIABLE INFORMATION IN TESTING, TRAINING, AND RESEARCH

Use [*Assignment: organization-defined techniques*] to minimize the use of personally identifiable information for research, testing, or training, in accordance with the privacy risk assessment.

Supplemental Guidance: Organizations can minimize the risk to an individual's privacy by using techniques such as de-identification or synthetic data. Limiting the use of personally identifiable information throughout the information life cycle when such information is not needed for research, testing, or training helps reduce the level of privacy risk created by a system.

Related Controls: PM-23.

References: NIST SP 800-188.

SI-13 PREDICTABLE FAILURE PREVENTION

Control:

a. Determine mean time to failure (MTTF) for [*Assignment: organization-defined system components*] in specific environments of operation; and

b. Provide substitute system components and a means to exchange active and standby components at [*Assignment: organization-defined MTTF substitution criteria*].

Supplemental Guidance: While MTTF is primarily a reliability issue, this control addresses potential failures of system components that provide security capability. Failure rates reflect installation-specific consideration, not industry-average. Organizations define the criteria for substitution of system components based on the MTTF value with consideration for resulting potential harm from component failures. Transfer of responsibilities between active and standby components does not compromise safety, operational readiness, or security capability. This includes, for example, preservation of system state variables. Standby components remain available at all times except for maintenance issues or recovery failures in progress.

Related Controls: CP-2, CP-10, CP-13, MA-2, MA-6, SC-6.

Control Enhancements:

(1) PREDICTABLE FAILURE PREVENTION | TRANSFERRING COMPONENT RESPONSIBILITIES

Takes 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.

Supplemental Guidance: None.

Related Controls: None.

(2) PREDICTABLE FAILURE PREVENTION | TIME LIMIT ON PROCESS EXECUTION WITHOUT SUPERVISION

[Withdrawn: Incorporated into SI-7(16)].

(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 ~~frequency~~*] if*percentage*] of the mean time to failure.

Supplemental Guidance: For example, if the MTTF for a system component is one hundred days and the organization-defined ***~~time period~~***.percentage is ninety percent, the manual transfer would occur after ninety days.

Related Controls: None.

(4) PREDICTABLE FAILURE PREVENTION | STANDBY COMPONENT INSTALLATION AND NOTIFICATION

~~The organization, if information~~If system component failures are detected:

(a) **~~Ensures~~Ensure that the standby components are successfully and transparently installed within [*Assignment: organization-defined time period*]; and**

(b) **[*Selection (one or more): ~~activates~~Activate* [*Assignment: organization-defined alarm*]; *Automatically shut down the system*~~]~~.; [*Assignment: organization-defined action*]].**

Supplemental Guidance: Automatic or manual transfer of components from standby to active mode can occur, for example, upon detection of component failures.

Related Controls: None.

(5) PREDICTABLE FAILURE PREVENTION | FAILOVER CAPABILITY

Provide [*Selection: real-time; near real-time*] [*Assignment: organization-defined failover capability*] *for the system.*

Supplemental Guidance: Failover refers to the automatic switchover to an alternate system upon the failure of the primary system. Failover capability includes, for example, incorporating mirrored system operations at alternate processing sites or periodic data mirroring at regular intervals defined by recovery time-periods of organizations.

Related Controls: CP-6, CP-7, CP-9.

References: None.

SI-14 NON-PERSISTENCE

Control: Implement non-persistent [*Assignment: organization-defined system components and services*] that are initiated in a known state and terminated [*Selection (one or more): upon end of session of use; periodically at* [*Assignment: organization-defined frequency*]].

Supplemental Guidance: This control mitigates risk from advanced persistent threats (APTs) by significantly 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 known state computing resource for a specific time-period that does not give adversaries sufficient time on target to exploit vulnerabilities in organizational systems and the environments in which those systems operate. Since the APT is a high-end, sophisticated threat regarding 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 in attempting to compromise or breach organizational systems.

Non-persistence can be achieved by refreshing system components, for example, by periodically re-imaging components or by using a variety of common virtualization techniques. Non-persistent services can be implemented 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. ~~In some instances,~~ Refreshes of critical components and services may be done periodically to hinder the ability of adversaries to exploit optimum windows of vulnerabilities.

Related Controls: SC-30, SC-34.

Control Enhancements:

(1) NON-PERSISTENCE | REFRESH FROM TRUSTED SOURCES

Obtain software and data employed during system component and service refreshes from [*Assignment: organization-defined trusted sources*].

Supplemental Guidance: Trusted sources include, for example, software and data from write-once, read-only media or from selected off-line secure storage facilities.

Related Controls: None.

References: None.

SI-15 INFORMATION OUTPUT FILTERING

Control: Validate information output from [*Assignment: organization-defined software programs and/or applications*] to ensure that the information is consistent with the expected content.

Supplemental Guidance: Certain types of ~~cyber~~ attacks ~~(e.g.,~~ including for example, SQL injections~~),~~ produce output results that are unexpected or inconsistent with the output results that would normally be expected from software programs or applications. This control enhancement focuses on detecting extraneous content, preventing such extraneous content from being displayed, and then alerting monitoring tools that anomalous behavior has been discovered.

Related Controls: SI-3, SI-4.

Control Enhancements:

(1) INFORMATION OUTPUT FILTERING | LIMIT PERSONALLY IDENTIFIABLE INFORMATION DISSEMINATION

Limit the dissemination of personally identifiable information to [*Assignment: organization-defined elements*] identified in the privacy risk assessment and consistent with authorized purposes.

Supplemental Guidance: Preventing the sharing of personally identifiable information outside of explicitly determined elements helps mitigate privacy risks that may arise from using such information to detect anomalous system behavior. Organizations weigh the risks created by using personally identifiable information for information output filtering (as either signature or heuristic information) against the security risks they help mitigate and the established privacy posture in the privacy program plan.

Related Controls: PA-2, PA-3, PM-18.

References: None.

SI-16 MEMORY PROTECTION

Control: Implement [*Assignment: organization-defined security safeguards*] to protect the system memory from unauthorized code execution.

Supplemental Guidance: Some adversaries launch attacks with the intent of executing code in non-executable regions of memory or in memory locations that are prohibited. Security safeguards employed to protect memory include, for example, data execution prevention and address space layout randomization. Data execution prevention safeguards can either be hardware-enforced or software-enforced with hardware enforcement providing the greater strength of mechanism.

Related Controls: AC-25, SC-3.

Control Enhancements: None.

References: None.

SI-17 FAIL-SAFE PROCEDURES

Control: Implement [*Assignment: organization-defined fail-safe procedures*] when [*Assignment: organization-defined failure conditions occur*].

Supplemental Guidance: Failure conditions include, for example, loss of communications among critical system components or between system components and operational facilities. Fail-safe procedures include, for example, alerting operator personnel and providing specific instructions on subsequent steps to take. These steps include, for example, doing nothing, reestablishing system settings, shutting down processes, restarting the system, or contacting designated organizational personnel.

Related Controls: CP-12, CP-13, SC-24, SI-13.

Control Enhancements: None.

References: None.

SI-18 INFORMATION DISPOSAL

Control: Use [*Assignment: organization-defined techniques or methods*] to dispose of, destroy, or erase information.

Supplemental Guidance: Disposal or destruction of information applies to originals as well as copies and archived records, including system logs that may contain personally identifiable information.

Related Controls: MP-6.

Control Enhancements: None.

References: None.

SI-19 DATA QUALITY OPERATIONS

Control:

a. Upon collection or creation of personally identifiable information, check for the accuracy, relevance, timeliness, impact, completeness, and de-identification of that information across the information life cycle; and

b. Check for and correct as necessary [*Assignment: organization-defined frequency*] and across the information life cycle:

   1. Inaccurate or outdated personally identifiable information;

   2. Personally identifiable information of incorrectly determined impact; or

   3. Incorrectly de-identified personally identifiable information.

Supplemental Guidance: The information life cycle includes information creation, collection, use, processing, storage, maintenance, dissemination, disclosure, disposition.

Related Controls: PM-25, SI-4, SI-20.

Control Enhancements:

(1) DATA QUALITY OPERATIONS | UPDATING AND CORRECTING PERSONALLY IDENTIFIABLE INFORMATION

Employ technical controls to correct personally identifiable information used in organizational programs and systems that is inaccurate or outdated, incorrectly determined regarding impact, or incorrectly de-identified.

Supplemental Guidance: Use of controls to improve data quality may inadvertently create privacy risks. Automated controls may connect to external or otherwise unrelated systems,

and the matching of records between these systems may create linkages with unintended consequences. Organizations assess and document these risks in their privacy impact assessment and make determinations that are in alignment with their privacy program plan.

Related Controls: PM-18, RA-8.

(2) DATA QUALITY OPERATIONS | DATA TAGS

Employ data tags to automate tracking of personally identifiable information across the information life cycle within organizational systems.

Supplemental Guidance: Data tags that contain information about retention dates, usage or disclosure policies, or other information pertaining to the management of personally identifiable information can support the use of automation tools to enforce relevant data management policies.

Related Controls: None.

(3) DATA QUALITY OPERATIONS | PERSONALLY IDENTIFIABLE INFORMATION COLLECTION

Collect personally identifiable information directly from the individual.

Supplemental Guidance: Organizations take reasonable steps to confirm the accuracy and relevance of personally identifiable information. These steps may include, for example, editing and validating addresses as they are collected or entered into systems using automated address verification look-up application programming interfaces. The types of measures taken to protect data quality are based on the nature and context of the personally identifiable information, how it is to be used, and how it was obtained. Measures taken to validate the accuracy of personally identifiable information used to make determinations about the rights, benefits, or privileges of individuals under federal programs may be more comprehensive than those used to validate less sensitive personally identifiable information. Additional steps may be necessary to validate personally identifiable information that is obtained from sources other than individuals or the authorized representatives of individuals.

Related Controls: None.

References: NIST Special Publication 800-188.

SI-20 DE-IDENTIFICATION

Control: Remove personally identifiable information from datasets.

Supplemental Guidance: Many datasets contain information about individuals that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records. Datasets may also contain other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. Personally identifiable information is removed from datasets by trained individuals when such information is not (or no longer) necessary to satisfy the requirements envisioned for the data. For example, if the dataset is only used to produce aggregate statistics, the identifiers that are not needed for producing those statistics are removed. Removing identifiers improves privacy protection, since information that is removed cannot be inadvertently disclosed or improperly used.

Related Controls: PM-23, PM-24, PM-25, SI-18, SI-19.

Control Enhancements:

(1) DE-IDENTIFICATION | COLLECTION

De-identify the dataset upon collection by not collecting personally identifiable information.

Supplemental Guidance: If a data source contains personally identifiable information but the information will not be used, the dataset can be de-identified upon creation by simply not collecting the data elements containing the personally identifiable information. For example, if an organization does not intend to use the social security number of an applicant, then application forms do not ask for a social security number.

Related Controls: None.

(2) DE-IDENTIFICATION | ARCHIVING

Refrain from archiving personally identifiable information elements if those elements in a dataset will not be needed after the dataset is archived.

Supplemental Guidance: 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.

Related Controls: None.

(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.

Supplemental Guidance: Prior to releasing a dataset, a data custodian considers the intended uses of the released dataset and determines if it is necessary to release personally identifiable information. If it is not necessary, the personally identifiable information can be removed using de-identification techniques.

Related Controls: None.

(4) DE-IDENTIFICATION | REMOVAL, MASKING, ENCRYPTION, HASHING, OR REPLACEMENT OF DIRECT IDENTIFIERS

Remove, mask, encrypt, hash, or replace direct identifiers in a dataset.

Supplemental Guidance: There are many possible processes for removing direct identifiers from a dataset. Columns in a dataset that contain a direct identifier can be removed. In masking, the direct identifier is transformed into a repeating character, for example, XXXXXX or 999999. Identifiers can be encrypted or hashed, so that the linked records remain linked. In the case of encryption or hashing, algorithms are employed that require the use of a key, including, for example, the Advanced Encryption Standard or a Hash-based Message Authentication Code. Implementations may use the same key for all identifiers or a different key for each identifier. Using a different key for each identifier provides for a higher degree of security and privacy. Identifiers can alternatively be replaced with a keyword, including for example, transforming "George Washington" to "PATIENT," or replaced with a realistic surrogate value, including for example, transforming "George Washington" to "Abraham Polk."

Related Controls: None.

(5) DE-IDENTIFICATION | STATISTICAL DISCLOSURE CONTROL

Manipulate numerical data, contingency tables, and statistical findings so that no person or organization is identifiable in the results of the analysis.

Supplemental Guidance: 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 publishes a monthly table with the number of minority students, and in January the school reports that it has 10-19 such students, but in March it reports that it has 20-29 such students, then it can be inferred that the student who enrolled in February was a minority.

Related Controls: None.

(6) DE-IDENTIFICATION | DIFFERENTIAL PRIVACY

Prevent disclosure of personally identifiable information by adding non-deterministic noise to the results of mathematical operations before the results are reported.

Supplemental Guidance: The mathematical definition for differential privacy holds that the result of a dataset analysis should be approximately the same before and after the addition or removal of a single data record (which is assumed to be the data from a single individual). In its most basic form, differential privacy applies only to online query systems. However, it can also be used to produce machine-learning statistical classifiers and synthetic data. Differential privacy comes at the cost of decreased accuracy of results, forcing organizations to quantify the trade-off between privacy protection and the overall accuracy, usefulness, and utility of the de-identified dataset. Non-deterministic noise can include, for example, adding small random values to the results of mathematical operations in dataset analysis.

Related Controls: None.

(7) DE-IDENTIFICATION | VALIDATED SOFTWARE

Perform de-identification using validated algorithms and software that is validated to implement the algorithms.

Supplemental Guidance: Algorithms that appear to remove personally identifiable information from a dataset may in fact leave information that is personally identifiable or data that are re-identifiable. Software that is claimed to implement a validated algorithm may contain bugs or may implement a different algorithm. Software may de-identify one type of data, for example, integers, but not another type of data, for example, floating point numbers. For these reasons, de-identification is performed using algorithms and software that are validated.

Related Controls: None.

(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.

Supplemental Guidance: A motivated intruder test is a test in which a person 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, financial resources, computational resources, data, and skills that intruders have at their disposal to conduct the tests. A motivated intruder test can identify if de-identification is insufficient. It can also be a useful diagnostic tool to assess if de-identification is likely to be sufficient; however, the test alone cannot prove that de-identification is sufficient.

Related Controls: None.

References: NIST Special Publication 800-188.