3.1 ACCESS CONTROL

Quick link to Access Control Summary Table

AC-1 POLICY AND PROCEDURES

Control:

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

   1. [*Selection (one or more): Organization-level; Mission/business process-level; System-level*] access control policy that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the access control policy and the associated access controls;

b. Designate an [*Assignment: organization-defined official*] to manage the development, documentation, and dissemination of the access control policy and procedures; and

c. Review and update the current access control:

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

   2. Procedures [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*].

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

Related Controls: IA-1, PM-9, PM-24, PS-8, SI-12.

Control Enhancements: None.

References: [OMB A-130], [SP 800-12], [SP 800-30], [SP 800-39], [SP 800-100], [IR 7874].

AC-2 ACCOUNT MANAGEMENT

Control:

a. Define and document the types of accounts allowed and specifically prohibited for use within the system;

b. Assign account managers;

c. Require [*Assignment: organization-defined prerequisites and criteria*] for group and role membership;

d. Specify:

   1. Authorized users of the system;

   2. Group and role membership; and

   3. Access authorizations (i.e., privileges) and [*Assignment: organization-defined attributes (as required)*] for each account;

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

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

g. Monitor the use of accounts;

h. Notify account managers and [*Assignment: organization-defined personnel or roles*] within:

   1. [*Assignment: organization-defined time period*] when accounts are no longer required;

   2. [*Assignment: organization-defined time period*] when users are terminated or transferred; and

   3. [*Assignment: organization-defined time period*] when system usage or need-to-know changes for an individual;

i. Authorize access to the system based on:

   1. A valid access authorization;

   2. Intended system usage; and

   3. [*Assignment: organization-defined attributes (as required)*];

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

k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and

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

Discussion: Examples of system account types include individual, shared, group, system, guest, anonymous, emergency, developer, temporary, and service. Identification of authorized system users and the specification of access privileges reflect the requirements in other controls in the security plan. Users requiring administrative privileges on system accounts receive additional scrutiny by organizational personnel responsible for approving such accounts and privileged access, including system owner, mission or business owner, senior agency information security officer, or senior agency official for privacy. Types of accounts that organizations may wish to prohibit due to increased risk include shared, group, emergency, anonymous, temporary, and guest accounts.

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

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

Related Controls: AC-3, AC-5, AC-6, AC-17, AC-18, AC-20, AC-24, AU-2, AU-12, CM-5, IA-2, IA-4, IA-5, IA-8, MA-3, MA-5, PE-2, PL-4, PS-2, PS-4, PS-5, PS-7, PT-2, PT-3, SC-7, SC-12, SC-13, SC-37.

Control Enhancements:

(1) ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT MANAGEMENT

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

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

Related Controls: None.

(2) ACCOUNT MANAGEMENT | AUTOMATED TEMPORARY AND EMERGENCY ACCOUNT MANAGEMENT

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

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

Related Controls: None.

(3) ACCOUNT MANAGEMENT | DISABLE ACCOUNTS

Disable accounts within [*Assignment: organization-defined time period*] when the accounts:

(a) Have expired;

(b) Are no longer associated with a user or individual;

(c) Are in violation of organizational policy; or

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

Discussion: Disabling expired, inactive, or otherwise anomalous accounts supports the concepts of least privilege and least functionality which reduce the attack surface of the system.

Related Controls: None.

(4) ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS

Automatically audit account creation, modification, enabling, disabling, and removal actions.

Discussion: Account management audit records are defined in accordance with AU-2 and reviewed, analyzed, and reported in accordance with AU-6.

Related Controls: AU-2, AU-6.

(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*].

Discussion: Inactivity logout is behavior- or policy-based and requires users to take physical action to log out when they are expecting inactivity longer than the defined period. Automatic enforcement of inactivity logout is addressed by AC-11.

Related Controls: AC-11.

(6) ACCOUNT MANAGEMENT | DYNAMIC PRIVILEGE MANAGEMENT

Implement [*Assignment: organization-defined dynamic privilege management capabilities*].

Discussion: In contrast to access control approaches that employ static accounts and predefined user privileges, dynamic access control approaches rely on runtime access control decisions facilitated by dynamic privilege management, such as attribute-based access control. While user identities remain relatively constant over time, user privileges typically change more frequently based on ongoing mission or business requirements and the operational needs of organizations. An example of dynamic privilege management is the immediate revocation of privileges from users as opposed to requiring that users terminate and restart their sessions to reflect changes in privileges. Dynamic privilege management can also include mechanisms that change user privileges based on dynamic rules as opposed to editing specific user profiles. Examples include automatic adjustments of user privileges if they are operating out of their normal work times, if their job function or assignment changes, or if systems are under duress or in emergency situations. Dynamic privilege management includes the effects of privilege changes, for example, when there are changes to encryption keys used for communications.

Related Controls: AC-16.

(7) ACCOUNT MANAGEMENT | PRIVILEGED USER ACCOUNTS

(a) Establish and administer privileged user accounts in accordance with [*Selection: a role-based access scheme; an attribute-based access scheme*];

(b) Monitor privileged role or attribute assignments;

(c) Monitor changes to roles or attributes; and

(d) Revoke access when privileged role or attribute assignments are no longer appropriate.

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

Related Controls: None.

(8) ACCOUNT MANAGEMENT | DYNAMIC ACCOUNT MANAGEMENT

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

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

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*].

Discussion: 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 CHANGE

[Withdrawn: Incorporated into AC-2k.]

(11) ACCOUNT MANAGEMENT | USAGE CONDITIONS

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

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

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*].

Discussion: Atypical usage includes accessing systems at certain times of the day or from locations that are not consistent with the normal usage patterns of individuals. Monitoring for atypical usage may reveal rogue behavior by individuals or an attack in progress. Account monitoring may inadvertently create privacy risks since data collected to identify atypical usage may reveal previously unknown information about the behavior of individuals. Organizations assess and document privacy risks from monitoring accounts for atypical

usage in their privacy impact assessment and make determinations that are in alignment with their privacy program plan.

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

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

Disable accounts of individuals within [*Assignment: organization-defined time period*] of discovery of [*Assignment: organization-defined significant risks*].

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

Related Controls: AU-6, SI-4.

References: [SP 800-162], [SP 800-178], [SP 800-192].

AC-3 ACCESS ENFORCEMENT

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

Discussion: Access control policies control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (i.e., devices, files, records, domains) in organizational systems. In addition to enforcing authorized access at the system level and recognizing that systems can host many applications and services in support of mission and business functions, access enforcement mechanisms can also be employed at the application and service level to provide increased information security and privacy. In contrast to logical access controls that are implemented within the system, physical access controls are addressed by the controls in the Physical and Environmental Protection (PE) family.

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, AT-2, AT-3, AU-9, CA-9, CM-5, CM-11, IA-2, IA-5, IA-6, IA-7, IA-11, MA-3, MA-4, MA-5, MP-4, PM-2, PS-3, PT-2, PT-3, SA-17, SC-2, SC-3, SC-4, SC-12, SC-13, SC-28, SC-31, SC-34, SI-4, SI-8.

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*].

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

Related Controls: CP-9, MP-6.

(3) ACCESS ENFORCEMENT | MANDATORY ACCESS CONTROL

Enforce [*Assignment: organization-defined mandatory access control policy*] over the set of covered subjects and objects specified in the policy, and where the policy:

(a) Is uniformly enforced across the covered subjects and objects within the system;

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

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

(2) Granting its privileges to other subjects;

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

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

(5) Changing the rules governing access control; and

(c) Specifies that [*Assignment: organization-defined subjects*] may explicitly be granted [*Assignment: organization-defined privileges*] such that they are not limited by any defined subset (or all) of the above constraints.

Discussion: Mandatory access control is a type of nondiscretionary access control. Mandatory access control policies constrain what actions subjects can take with information obtained from objects for which they have already been granted access. This prevents the subjects from passing the information to unauthorized subjects and objects. Mandatory access control policies constrain actions that subjects can take with respect to the propagation of access control privileges; that is, a subject with a privilege cannot pass that privilege to other subjects. The policy is uniformly enforced over all subjects and objects to which the system has control. Otherwise, the access control policy can be circumvented. This enforcement is provided by an implementation that meets the reference monitor concept as described in AC-25. The policy is bounded by the system (i.e., once the information is passed outside of the control of the system, additional means may be required to ensure that the constraints on the information remain in effect).

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

Related Controls: SC-7.

(4) ACCESS ENFORCEMENT | DISCRETIONARY ACCESS CONTROL

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

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

(b) Grant its privileges to other subjects;

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

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

(e) Change the rules governing access control.

Discussion: When discretionary access control policies are implemented, subjects are not constrained with regard to what actions they can take with information for which they have already been granted access. Thus, subjects that have been granted access to information are not prevented from passing the information to other subjects or objects (i.e., subjects have the discretion to pass). Discretionary access control can operate in conjunction with mandatory access control as described in AC-3(3) and AC-3(15). A subject that is constrained in its operation by mandatory access control policies can still operate under the less rigorous constraints of discretionary access control. Therefore, while AC-3(3) imposes constraints that prevent a subject from passing information to another subject operating at a different impact or classification level, AC-3(4) permits the subject to pass the information to any subject at the same impact or classification level. The policy is bounded by the system. Once the information is passed outside of system control, additional means may be required to ensure that the constraints remain in effect. While traditional definitions of discretionary access control require identity-based access control, that limitation is not required for this particular use of discretionary access control.

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.

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

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*].

Discussion: Role-based access control (RBAC) is an access control policy that enforces access to objects and system functions based on the defined role (i.e., job function) of the subject. Organizations can create specific roles based on job functions and the authorizations (i.e., privileges) to perform needed operations on the systems associated with the organization-defined roles. When users are assigned to specific roles, they inherit the authorizations or privileges defined for those roles. RBAC simplifies privilege administration for organizations because privileges are not assigned directly to every user (which can be a large number of individuals) but are instead acquired through role assignments. RBAC can also increase

privacy and security risk if individuals assigned to a role are given access to information beyond what they need to support organizational missions or business functions. RBAC can be implemented as a mandatory or discretionary form of access control. For organizations implementing RBAC with mandatory access controls, the requirements in AC-3(3) define the scope of the subjects and objects covered by the policy.

Related Controls: None.

(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*].

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

Related Controls: None.

(9) ACCESS ENFORCEMENT | CONTROLLED RELEASE

Release information outside of the system only if:

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

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

Discussion: Organizations can only directly protect information when it resides within the system. Additional controls may be needed to ensure that organizational information is adequately protected once it is transmitted outside of the system. In situations where the system is unable to determine the adequacy of the protections provided by external entities, as a mitigation measure, organizations procedurally determine whether the external systems are providing adequate controls. The means used to determine the adequacy of controls provided by external systems include conducting periodic assessments (inspections/tests), establishing agreements between the organization and its counterpart organizations, or some other process. The means used by external entities to protect the information received need not be the same as those used by the organization, but the means employed are sufficient to provide consistent adjudication of the security and privacy policy to protect the information and individuals' privacy.

Controlled release of information requires systems to implement technical or procedural means to validate the information prior to releasing it to external systems. For example, if the system passes information to a system controlled by another organization, technical means are employed to validate that the security and privacy attributes associated with the exported information are appropriate for the receiving system. Alternatively, if the system passes information to a printer in organization-controlled space, procedural means can be employed to ensure that only authorized individuals gain access to the printer.

Related Controls: CA-3, PT-7, PT-8, SA-9, 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*].

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

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

(11) ACCESS ENFORCEMENT | RESTRICT ACCESS TO SPECIFIC INFORMATION TYPES

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

Discussion: Restricting access to specific information is intended to provide flexibility regarding access control of specific information types within a system. For example, role-based access could be employed to allow access to only a specific type of personally identifiable information within a database rather than allowing access to the database in its entirety. Other examples include restricting access to cryptographic keys, authentication information, and selected system information.

Related Controls: CM-8, CM-12, CM-13, PM-5.

(12) ACCESS ENFORCEMENT | ASSERT AND ENFORCE APPLICATION ACCESS

(a) Require applications to assert, as part of the installation process, the access needed to the following system applications and functions: [*Assignment: organization-defined system applications and functions*];

(b) Provide an enforcement mechanism to prevent unauthorized access; and

(c) Approve access changes after initial installation of the application.

Discussion: Asserting and enforcing application access is intended to address applications that need to access existing system applications and functions, including user contacts, global positioning systems, cameras, keyboards, microphones, networks, phones, or other files.

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*].

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

Related Controls: None.

(14) ACCESS ENFORCEMENT | INDIVIDUAL ACCESS

Provide [*Assignment: organization-defined mechanisms*] to enable individuals to have access to the following elements of their personally identifiable information: [*Assignment: organization-defined elements*].

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

Related Controls: IA-8, PM-22, PM-20, PM-21, PT-6.

(15) ACCESS ENFORCEMENT | DISCRETIONARY AND MANDATORY ACCESS CONTROL

(a) Enforce [*Assignment: organization-defined mandatory access control policy*] over the set of covered subjects and objects specified in the policy; and

(b) Enforce [*Assignment: organization-defined discretionary access control policy*] over the set of covered subjects and objects specified in the policy.

Discussion: Simultaneously implementing a mandatory access control policy and a discretionary access control policy can provide additional protection against the unauthorized execution of code by users or processes acting on behalf of users. This helps prevent a single compromised user or process from compromising the entire system.

Related Controls: SC-2, SC-3, AC-4.

References: [PRIVACT], [OMB A-130], [SP 800-57-1], [SP 800-57-2], [SP 800-57-3], [SP 800-162], [SP 800-178], [IR 7874].

AC-4 INFORMATION FLOW ENFORCEMENT

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

Discussion: Information flow control regulates where information can travel within a system and between systems (in contrast to who is allowed to access the information) and without regard to subsequent accesses to that information. Flow control restrictions include blocking external traffic that claims to be from within the organization, keeping export-controlled information from being transmitted in the clear to the Internet, restricting web requests that are not from the internal web proxy server, and limiting information transfers between organizations based on data structures and content. Transferring information between organizations may require an agreement specifying how the information flow is enforced (see CA-3). Transferring information between systems in different security or privacy domains with different security or privacy policies introduces the risk that such transfers violate one or more domain security or privacy policies. In such situations, information owners/stewards provide guidance at designated policy enforcement points between connected systems. Organizations consider mandating specific architectural solutions to enforce specific security and privacy policies. Enforcement includes prohibiting information transfers between connected systems (i.e., allowing access only), verifying write permissions before accepting information from another security or privacy domain or connected system, employing hardware mechanisms to enforce one-way information

flows, and implementing trustworthy regrading mechanisms to reassign security or privacy attributes and labels.

Organizations commonly employ information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations within systems and between connected systems. Flow control is based on the characteristics of the information and/or the information path. Enforcement occurs, for example, in boundary protection devices that employ rule sets or establish configuration settings that restrict system services, provide a packet-filtering capability based on header information, or provide a message-filtering capability based on message content. Organizations also consider the trustworthiness of filtering and/or inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement. Control enhancements 3 through 32 primarily address cross-domain solution needs that focus on more advanced filtering techniques, in-depth analysis, and stronger flow enforcement mechanisms implemented in cross-domain products, such as high-assurance guards. Such capabilities are generally not available in commercial off-the-shelf products. Information flow enforcement also applies to control plane traffic (e.g., routing and DNS).

Related Controls: AC-3, AC-6, AC-16, AC-17, AC-19, AC-21, AU-10, CA-3, CA-9, CM-7, PL-9, PM-24, SA-17, SC-4, SC-7, SC-16, SC-31.

Control Enhancements:

(1) INFORMATION FLOW ENFORCEMENT | OBJECT SECURITY AND PRIVACY ATTRIBUTES

Use [*Assignment: organization-defined security and privacy attributes*] associated with [*Assignment: organization-defined information, source, and destination objects*] to enforce [*Assignment: organization-defined information flow control policies*] as a basis for flow control decisions.

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

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.

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

Related Controls: SC-39.

(3) INFORMATION FLOW ENFORCEMENT | DYNAMIC INFORMATION FLOW CONTROL

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

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

Related Controls: SI-4.

(4) INFORMATION FLOW ENFORCEMENT | FLOW CONTROL OF ENCRYPTED INFORMATION

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

Discussion: Flow control mechanisms include content checking, security policy filters, and data type identifiers. The term encryption is extended to cover encoded data not recognized by filtering mechanisms.

Related Controls: SI-4.

(5) INFORMATION FLOW ENFORCEMENT | EMBEDDED DATA TYPES

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

Discussion: Embedding data types within other data types may result in reduced flow control effectiveness. Data type embedding includes inserting files as objects within other files and using compressed or archived data types that may include multiple embedded data types. Limitations on data type embedding consider the levels of embedding and prohibit levels of data type embedding that are beyond the capability of the inspection tools.

Related Controls: None.

(6) INFORMATION FLOW ENFORCEMENT | METADATA

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

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

Related Controls: AC-16, SI-7.

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

Enforce one-way information flows through hardware-based flow control mechanisms.

Discussion: One-way flow mechanisms may also be referred to as a unidirectional network, unidirectional security gateway, or data diode. One-way flow mechanisms can be used to prevent data from being exported from a higher impact or classified domain or system while permitting data from a lower impact or unclassified domain or system to be imported.

Related Controls: None.

(8) INFORMATION FLOW ENFORCEMENT | SECURITY AND PRIVACY POLICY FILTERS

(a) Enforce information flow control using [*Assignment: organization-defined security or privacy policy filters*] as a basis for flow control decisions for [*Assignment: organization-defined information flows*]; and

(b) [*Selection (one or more): Block; Strip; Modify; Quarantine*] data after a filter processing failure in accordance with [*Assignment: organization-defined security or privacy policy*].

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

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*].

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

Related Controls: None.

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

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

Discussion: For example, as allowed by the system authorization, administrators can enable security or privacy policy filters to accommodate approved data types. Administrators also have the capability to select the filters that are executed on a specific data flow based on the type of data that is being transferred, the source and destination security domains, and other security or privacy relevant features, as needed.

Related Controls: None.

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

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

Discussion: Documentation contains detailed information for configuring security or privacy policy filters. For example, administrators can configure security or privacy policy filters to include the list of inappropriate words that security or privacy policy mechanisms check in accordance with the definitions provided by organizations.

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.

Discussion: Data type identifiers include filenames, file types, file signatures or tokens, and multiple internal file signatures or tokens. Systems only allow transfer of data that is compliant with data type format specifications. Identification and validation of data types is based on defined specifications associated with each allowed data format. The filename and number alone are not used for data type identification. Content is validated syntactically and semantically against its specification to ensure that it is the proper data type.

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.

Discussion: Decomposing information into policy-relevant subcomponents prior to information transfer facilitates policy decisions on source, destination, certificates, classification, attachments, and other security- or privacy-related component differentiators. Policy enforcement mechanisms apply filtering, inspection, and/or sanitization rules to the policy-relevant subcomponents of information to facilitate flow enforcement prior to transferring such information to different security domains.

Related Controls: None.

(14) INFORMATION FLOW ENFORCEMENT | SECURITY OR PRIVACY POLICY FILTER CONSTRAINTS

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

Discussion: Data structure and content restrictions reduce the range of potential malicious or unsanctioned content in cross-domain transactions. Security or privacy policy filters that restrict data structures include restricting file sizes and field lengths. Data content policy filters include encoding formats for character sets, restricting character data fields to only contain alpha-numeric characters, prohibiting special characters, and validating schema structures.

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: organization-defined unsanctioned information*] and prohibit the transfer of such information in accordance with the [*Assignment: organization-defined security or privacy policy*].

Discussion: Unsanctioned information includes malicious code, information that is inappropriate for release from the source network, or executable code that could disrupt or harm the services or systems on the destination network.

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.

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

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

(18) INFORMATION FLOW ENFORCEMENT | SECURITY ATTRIBUTE BINDING

[Withdrawn: Incorporated into AC-16.]

(19) INFORMATION FLOW ENFORCEMENT | VALIDATION OF METADATA

When transferring information between different security domains, implement [*Assignment: organization-defined security or privacy policy filters*] on metadata.

Discussion: All information (including metadata and the data to which the metadata applies) is subject to filtering and inspection. Some organizations distinguish between metadata and data payloads (i.e., only the data to which the metadata is bound). Other organizations do not make such distinctions and consider metadata and the data to which the metadata applies to be part of the payload.

Related Controls: None.

(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.

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

Related Controls: None.

(21) INFORMATION FLOW ENFORCEMENT | PHYSICAL OR 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*].

Discussion: Enforcing the separation of information flows associated with defined types of data can enhance protection by ensuring that information is not commingled while in transit and by enabling flow control by transmission paths that are not otherwise achievable. Types of separable information include inbound and outbound communications traffic, service requests and responses, and information of differing security impact or classification levels.

Related Controls: SC-32.

(22) INFORMATION FLOW ENFORCEMENT | ACCESS ONLY

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

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

Related Controls: None.

(23) INFORMATION FLOW ENFORCEMENT | MODIFY NON-RELEASABLE INFORMATION

When transferring information between different security domains, modify non-releasable information by implementing [*Assignment: organization-defined modification action*].

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

Related Controls: None.

(24) INFORMATION FLOW ENFORCEMENT | INTERNAL NORMALIZED FORMAT

When transferring information between different security domains, parse incoming data into an internal normalized format and regenerate the data to be consistent with its intended specification.

Discussion: Converting data into normalized forms is one of most of effective mechanisms to stop malicious attacks and large classes of data exfiltration.

Related Controls: None.

(25) INFORMATION FLOW ENFORCEMENT | DATA SANITIZATION

When transferring information between different security domains, sanitize data to minimize [*Selection (one or more): delivery of malicious content, command and control of malicious code, malicious code augmentation, and steganography encoded data; spillage of sensitive information*] in accordance with [*Assignment: organization-defined policy*]].

Discussion: Data sanitization is the process of irreversibly removing or destroying data stored on a memory device (e.g., hard drives, flash memory/solid state drives, mobile devices, CDs, and DVDs) or in hard copy form.

Related Controls: MP-6.

(26) INFORMATION FLOW ENFORCEMENT | AUDIT FILTERING ACTIONS

When transferring information between different security domains, record and audit content filtering actions and results for the information being filtered.

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

Related Controls: AU-2, AU-3, AU-12.

(27) INFORMATION FLOW ENFORCEMENT | REDUNDANT/INDEPENDENT FILTERING MECHANISMS

When transferring information between different security domains, implement content filtering solutions that provide redundant and independent filtering mechanisms for each data type.

Discussion: Content filtering is the process of inspecting information as it traverses a cross-domain solution and determines if the information meets a predefined policy. Redundant

and independent content filtering eliminates a single point of failure filtering system. Independence is defined as the implementation of a content filter that uses a different code base and supporting libraries (e.g., two JPEG filters using different vendors' JPEG libraries) and multiple, independent system processes.

Related Controls: None.

(28) INFORMATION FLOW ENFORCEMENT | LINEAR FILTER PIPELINES

When transferring information between different security domains, implement a linear content filter pipeline that is enforced with discretionary and mandatory access controls.

Discussion: Content filtering is the process of inspecting information as it traverses a cross-domain solution and determines if the information meets a predefined policy. The use of linear content filter pipelines ensures that filter processes are non-bypassable and always invoked. In general, the use of parallel filtering architectures for content filtering of a single data type introduces bypass and non-invocation issues.

Related Controls: None.

(29) INFORMATION FLOW ENFORCEMENT | FILTER ORCHESTRATION ENGINES

When transferring information between different security domains, employ content filter orchestration engines to ensure that:

(a) Content filtering mechanisms successfully complete execution without errors; and

(b) Content filtering actions occur in the correct order and comply with [*Assignment: organization-defined policy*].

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

Related Controls: None.

(30) INFORMATION FLOW ENFORCEMENT | FILTER MECHANISMS USING MULTIPLE PROCESSES

When transferring information between different security domains, implement content filtering mechanisms using multiple processes.

Discussion: The use of multiple processes to implement content filtering mechanisms reduces the likelihood of a single point of failure.

Related Controls: None.

(31) INFORMATION FLOW ENFORCEMENT | FAILED CONTENT TRANSFER PREVENTION

When transferring information between different security domains, prevent the transfer of failed content to the receiving domain.

Discussion: Content that failed filtering checks can corrupt the system if transferred to the receiving domain.

Related Controls: None.

(32) INFORMATION FLOW ENFORCEMENT | PROCESS REQUIREMENTS FOR INFORMATION TRANSFER

When transferring information between different security domains, the process that transfers information between filter pipelines:

(a) Does not filter message content;

(b) Validates filtering metadata;

(c) Ensures the content associated with the filtering metadata has successfully completed filtering; and

(d) Transfers the content to the destination filter pipeline.

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

Related Controls: None.

References: [SP-800-160-1], [SP 800-162], [SP 800-178], [IR 8112].

AC-5 SEPARATION OF DUTIES

Control:

a. Identify and document [*Assignment: organization-defined duties of individuals requiring separation*]; and

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

Discussion: Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes dividing mission or business functions and support functions among different individuals or roles, conducting system support functions with different individuals, and ensuring that security personnel who administer access control functions do not also administer audit functions. Because separation of duty violations can span systems and application domains, organizations consider the entirety of systems and system components when developing policy on separation of duties. Separation of duties is enforced through the account management activities in AC-2, access control mechanisms in AC-3, and identity management activities in IA-2, IA-4, and IA-12.

Related Controls: AC-2, AC-3, AC-6, AU-9, CM-5, CM-11, CP-9, IA-2, IA-4, IA-5, IA-12, MA-3, MA-5, PS-2, SA-8, SA-17.

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) that are necessary to accomplish assigned organizational tasks.

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

Related Controls: AC-2, AC-3, AC-5, AC-16, CM-5, CM-11, PL-2, PM-12, SA-8, SA-15, SA-17, SC-38.

Control Enhancements:

(1) LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS

Authorize access for [*Assignment: organization-defined individuals or roles*] to:

(a) [*Assignment: organization-defined security functions (deployed in hardware, software, and firmware)*]; and

(b) [*Assignment: organization-defined security-relevant information*].

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

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.

Discussion: Requiring the use of non-privileged accounts when accessing nonsecurity functions limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations implement access control policies, such as role-based access control, and where a change of role provides the same degree of assurance in the change of access authorizations for the user and the processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account.

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.

Discussion: 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.

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

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*].

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

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.

Discussion: An organizational user is an employee or an individual considered by the organization to have the equivalent status of an employee. Organizational users include contractors, guest researchers, or individuals detailed from other organizations. A non-organizational user is a user who is not an organizational user. Policies and procedures for granting equivalent status of employees to individuals include a need-to-know, citizenship, and the relationship to the organization.

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.

Discussion: The need for certain assigned user privileges may change over time to reflect changes in organizational mission and business functions, environments of operation, technologies, or threats. A periodic review of assigned user privileges is necessary to determine if the rationale for assigning such privileges remains valid. If the need cannot be revalidated, organizations take appropriate corrective actions.

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*].

Discussion: In certain situations, software applications or programs need to execute with elevated privileges to perform required functions. However, depending on the software functionality and configuration, if the privileges required for execution are at a higher level than the privileges assigned to organizational users invoking such applications or programs, those users may indirectly be provided with greater privileges than assigned.

Related Controls: None.

(9) LEAST PRIVILEGE | LOG USE OF PRIVILEGED FUNCTIONS

Log the execution of privileged functions.

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

Related Controls: AU-2, AU-3, AU-12.

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

Prevent non-privileged users from executing privileged functions.

Discussion: Privileged functions include disabling, circumventing, or altering implemented security or privacy controls, establishing system accounts, performing system integrity checks, and administering cryptographic key management activities. Non-privileged users are individuals who do not possess appropriate authorizations. Privileged functions that require protection from non-privileged users include circumventing intrusion detection and

prevention mechanisms or malicious code protection mechanisms. Preventing non-privileged users from executing privileged functions is enforced by AC-3.

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

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

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.

Discussion: A mobile device is a computing device that has a small form factor such that it can be carried by a single individual; is designed to operate without a physical connection; possesses local, non-removable or removable data storage; and includes a self-contained power source. Purging or wiping the device applies only to mobile devices for which the organization-defined number of unsuccessful logons occurs. The logon is to the mobile

device, not to any one account on the device. Successful logons to accounts on mobile devices reset the unsuccessful logon count to zero. Purging or wiping may be unnecessary if the information on the device is protected with sufficiently strong encryption mechanisms.

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*].

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

Related Controls: IA-3.

(4) UNSUCCESSFUL LOGON ATTEMPTS | USE OF ALTERNATE AUTHENTICATION FACTOR

(a) Allow the use of [*Assignment: organization-defined authentication factors*] that are different from the primary authentication factors after the number of organization-defined consecutive invalid logon attempts have been exceeded; and

(b) Enforce a limit of [*Assignment: organization-defined number*] consecutive invalid logon attempts through use of the alternative factors by a user during a [*Assignment: organization-defined time period*].

Discussion: The use of alternate authentication factors supports the objective of availability and allows a user who has inadvertently been locked out to use additional authentication factors to bypass the lockout.

Related Controls: IA-3.

References: [SP 800-63-3], [SP 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, regulations, policies, standards, and guidelines and state that:

   1. Users are accessing a U.S. Government system;
   2. System usage may be monitored, recorded, and subject to audit;
   3. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and
   4. Use of the system indicates consent to monitoring and recording;

b. Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system; and

c. For publicly accessible systems:

   1. Display system use information [*Assignment: organization-defined conditions*], before granting further access to the publicly accessible system;
   2. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and

3. Include a description of the authorized uses of the system.

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

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

Control Enhancements: None.

References: None.

AC-9 PREVIOUS LOGON NOTIFICATION

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

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

Related Controls: AC-7, PL-4.

Control Enhancements:

(1) PREVIOUS LOGON NOTIFICATION | UNSUCCESSFUL LOGONS

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

Discussion: Information about the number of unsuccessful logon attempts since the last successful logon allows the user to recognize if the number of unsuccessful logon attempts is consistent with the user's actual logon attempts.

Related Controls: None.

(2) PREVIOUS LOGON NOTIFICATION | SUCCESSFUL AND UNSUCCESSFUL LOGONS

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

Discussion: Information about the number of successful and unsuccessful logon attempts within a specified time period allows the user to recognize if the number and type of logon attempts are consistent with the user's actual logon attempts.

Related Controls: None.

(3) PREVIOUS LOGON NOTIFICATION | NOTIFICATION OF ACCOUNT CHANGES

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

Discussion: Information about changes to security-related account characteristics within a specified time period allows users to recognize if changes were made without their knowledge.

Related Controls: None.

(4) PREVIOUS LOGON NOTIFICATION | ADDITIONAL LOGON INFORMATION

Notify the user, upon successful logon, of the following additional information: [*Assignment: organization-defined additional information*].

Discussion: Organizations can specify additional information to be provided to users upon logon, including the location of the last logon. User location is defined as information that can be determined by systems, such as Internet Protocol (IP) addresses from which network logons occurred, notifications of local logons, or device identifiers.

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*].

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

Related Controls: SC-23.

Control Enhancements: None.

References: None.

AC-11 DEVICE LOCK

Control:

a. Prevent further access to the system by [*Selection (one or more): initiating a device lock after* [*Assignment: organization-defined time period*] *of inactivity; requiring the user to initiate a device lock before leaving the system unattended*]; and

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

Discussion: Device locks are temporary actions taken to prevent logical access to organizational systems when users stop work and move away from the immediate vicinity of those systems but do not want to log out because of the temporary nature of their absences. Device locks can be implemented at the operating system level or at the application level. A proximity lock may be used to initiate the device lock (e.g., via a Bluetooth-enabled device or dongle). User-initiated device locking is behavior or policy-based and, as such, requires users to take physical action to initiate the device lock. Device locks are not an acceptable substitute for logging out of systems, such as when organizations require users to log out at the end of workdays.

Related Controls: AC-2, AC-7, IA-11, PL-4.

Control Enhancements:

(1) DEVICE LOCK | PATTERN-HIDING DISPLAYS

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

Discussion: The pattern-hiding display can include static or dynamic images, such as patterns used with screen savers, photographic images, solid colors, clock, battery life indicator, or a blank screen with the caveat that controlled unclassified information is not displayed.

Related Controls: None.

References: None.

AC-12 SESSION TERMINATION

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

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

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

Control Enhancements:

(1) SESSION TERMINATION | USER-INITIATED LOGOUTS

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

Discussion: Information resources to which users gain access via authentication include local workstations, databases, and password-protected websites or web-based services.

Related Controls: None.

(2) SESSION TERMINATION | TERMINATION MESSAGE

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

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

Related Controls: None.

(3) SESSION TERMINATION | TIMEOUT WARNING MESSAGE

Display an explicit message to users indicating that the session will end in [*Assignment: organization-defined time until end of session*].

Discussion: To increase usability, notify users of pending session termination and prompt users to continue the session. The pending session termination time period is based on the parameters defined in the AC-12 base control.

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 mission and business functions; and

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

Discussion: Specific user actions may be permitted without identification or authentication if organizations determine that identification and authentication are not required for the specified user actions. Organizations may allow a limited number of user actions without identification or authentication, including when individuals access public websites or other publicly accessible federal systems, when individuals use mobile phones to receive calls, or when facsimiles are received. Organizations identify actions that normally require identification or authentication but may, under certain circumstances, allow identification or authentication mechanisms to be bypassed. Such bypasses may occur, for example, via a software-readable physical switch that commands bypass of the logon functionality and is protected from accidental or unmonitored use. Permitting actions without identification or authentication does not apply to situations where identification and authentication have already occurred and are not repeated but rather to situations where identification and authentication have not yet occurred. Organizations may decide that there are no user actions that can be performed on organizational systems without identification and authentication, and therefore, the value for the assignment operation can be "none."

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*] with [*Assignment: organization-defined security and privacy attribute values*] for information in storage, in process, and/or in transmission;

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

c. Establish the following permitted security and privacy attributes from the attributes defined in AC-16a for [*Assignment: organization-defined systems*]: [*Assignment: organization-defined security and privacy attributes*];

d. Determine the following permitted attribute values or ranges for each of the established attributes: [*Assignment: organization-defined attribute values or ranges for established attributes*];

e. Audit changes to attributes; and

f. Review [*Assignment: organization-defined security and privacy attributes*] for applicability [*Assignment: organization-defined frequency*].

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

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

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

Related Controls: AC-3, AC-4, AC-6, AC-21, AC-25, AU-2, AU-10, MP-3, PE-22, PT-2, PT-3, PT-4, SC-11, SC-16, SI-12, SI-18.

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 the following security and privacy policies as information is created and combined: [*Assignment: organization-defined security and privacy policies*].

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

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.

Discussion: The content or assigned values of attributes can directly affect the ability of individuals to access organizational information. Therefore, it is important for systems to be able to limit the ability to create or modify attributes to authorized individuals.

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*].

Discussion: Maintaining the association and integrity of security and privacy attributes to subjects and objects with sufficient assurance helps to ensure that the attribute associations can be used as the basis of automated policy actions. The integrity of specific items, such as security configuration files, may be maintained through the use of an integrity monitoring mechanism that detects anomalies and changes that deviate from "known good" baselines. Automated policy actions include retention date expirations, access control decisions, information flow control decisions, and information disclosure decisions.

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).

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

Related Controls: None.

(5) SECURITY AND PRIVACY ATTRIBUTES | ATTRIBUTE DISPLAYS ON OBJECTS TO BE OUTPUT

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

Discussion: System outputs include printed pages, screens, or equivalent items. System output devices include printers, notebook computers, video displays, smart phones, and tablets. To mitigate the risk of unauthorized exposure of information (e.g., shoulder surfing), the outputs display full attribute values when unmasked by the subscriber.

Related Controls: None.

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

Require personnel to associate and maintain the association of [*Assignment: organization-defined security and privacy attributes*] with [*Assignment: organization-defined subjects and objects*] in accordance with [*Assignment: organization-defined security and privacy policies*].

Discussion: Maintaining attribute association requires individual users (as opposed to the system) to maintain associations of defined 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.

Discussion: To enforce security and privacy policies across multiple system components in distributed systems, organizations provide a consistent interpretation of security and privacy attributes employed in access enforcement and flow enforcement decisions. Organizations can establish agreements and processes to help ensure that distributed system components implement attributes with consistent interpretations in automated access enforcement and flow enforcement actions.

Related Controls: None.

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

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

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

Related Controls: SC-12, SC-13.

(9) SECURITY AND PRIVACY ATTRIBUTES | ATTRIBUTE REASSIGNMENT — REGRADING MECHANISMS

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

Discussion: A regrading mechanism is a trusted process authorized to re-classify and re-label data in accordance with a defined policy exception. Validated regrading mechanisms are

used by organizations to provide the requisite levels of assurance for attribute reassignment activities. The validation is facilitated by ensuring that regrading mechanisms are single purpose and of limited function. Since security and privacy attribute changes can directly affect policy enforcement actions, implementing trustworthy regrading mechanisms is necessary to help ensure that such mechanisms perform in a consistent and correct mode of operation.

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.

Discussion: The content or assigned values of security and privacy attributes can directly affect the ability of individuals to access organizational information. Thus, it is important for systems to be able to limit the ability to create or modify the type and value of attributes available for association with subjects and objects to authorized individuals only.

Related Controls: None.

References: [OMB A-130], [FIPS 140-3], [FIPS 186-4], [SP 800-162], [SP 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 each type of remote access to the system prior to allowing such connections.

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

Related Controls: AC-2, AC-3, AC-4, AC-18, AC-19, AC-20, CA-3, CM-10, IA-2, IA-3, IA-8, MA-4, PE-17, PL-2, PL-4, SC-10, SC-12, SC-13, SI-4.

Control Enhancements:

(1) REMOTE ACCESS | MONITORING AND CONTROL

Employ automated mechanisms to monitor and control remote access methods.

Discussion: Monitoring and control of remote access methods allows organizations to detect attacks and help ensure compliance with remote access policies by auditing the connection activities of remote users on a variety of system components, including servers,

notebook computers, workstations, smart phones, and tablets. Audit logging for remote access is enforced by AU-2. Audit events are defined in AU-2a.

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.

Discussion: Virtual private networks can be used to protect the confidentiality and integrity of remote access sessions. Transport Layer Security (TLS) is an example of a cryptographic protocol that provides end-to-end communications security over networks and is used for Internet communications and online transactions.

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

(3) REMOTE ACCESS | MANAGED ACCESS CONTROL POINTS

Route remote accesses through authorized and managed network access control points.

Discussion: Organizations consider the Trusted Internet Connections (TIC) initiative [DHS TIC] requirements for external network connections since limiting the number of access control points for remote access reduces attack surfaces.

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 in a format that provides assessable evidence and for the following needs: [*Assignment: organization-defined needs*]; and

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

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

Related Controls: AC-6, SC-12, SC-13.

(5) REMOTE ACCESS | MONITORING FOR UNAUTHORIZED CONNECTIONS

[Withdrawn: Incorporated into SI-4.]

(6) REMOTE ACCESS | PROTECTION OF MECHANISM INFORMATION

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

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

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

Discussion: The speed of system disconnect or disablement varies based on the criticality of missions or business functions and the need to eliminate immediate or future remote access to systems.

Related Controls: None.

(10) REMOTE ACCESS | AUTHENTICATE REMOTE COMMANDS

Implement [*Assignment: organization-defined mechanisms*] to authenticate [*Assignment: organization-defined remote commands*].

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

Related Controls: SC-12, SC-13, SC-23.

References: [SP 800-46], [SP 800-77], [SP 800-113], [SP 800-114], [SP 800-121], [IR 7966].

AC-18 WIRELESS ACCESS

Control:

a. Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access; and

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

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

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.

Discussion: Wireless networking capabilities represent a significant potential vulnerability that can be exploited by adversaries. To protect systems with wireless access points, strong authentication of users and devices along with strong encryption can reduce susceptibility to threats by adversaries involving wireless technologies.

Related Controls: SC-8, SC-12, 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 embedded within system components prior to issuance and deployment.

Discussion: Wireless networking capabilities that are embedded within system components represent a significant potential vulnerability that can be exploited by adversaries. Disabling wireless capabilities when not needed for essential organizational missions or functions can reduce susceptibility to threats by adversaries involving wireless technologies.

Related Controls: None.

(4) WIRELESS ACCESS | RESTRICT CONFIGURATIONS BY USERS

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

Discussion: Organizational authorizations to allow selected users to configure wireless networking capabilities 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.

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

Related Controls: PE-19.

References: [SP 800-94], [SP 800-97].

AC-19 ACCESS CONTROL FOR MOBILE DEVICES

Control:

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

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

Discussion: A mobile device is a computing device that has a small form factor such that it can easily be carried by a single individual; is designed to operate without a physical connection; possesses local, non-removable or removable data storage; and includes a self-contained power source. Mobile device functionality may also include voice communication capabilities, on-board sensors that allow the device to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones and tablets. Mobile devices are typically associated with a single individual. The processing, storage, and transmission capability of the mobile device may be comparable to or merely a subset of notebook/desktop systems, depending on the nature and intended purpose of the device. Protection and control of mobile devices is behavior or policy-based and requires users to take physical action to protect and control such devices when outside of controlled areas. Controlled areas are spaces for which organizations provide physical or procedural controls to meet the requirements established for protecting information and systems.

Due to the large variety of mobile devices with different characteristics and capabilities, organizational restrictions may vary for the different classes or types of such devices. Usage restrictions and specific implementation guidance for mobile devices include configuration management, device identification and authentication, implementation of mandatory protective software, scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware.

Usage restrictions and authorization to connect may vary among organizational systems. For example, the organization may authorize the connection of mobile devices to its network and impose a set of usage restrictions, while a system owner may withhold authorization for mobile device connection to specific applications or impose additional usage restrictions before allowing mobile device connections to a system. Adequate security for mobile devices goes beyond the requirements specified in AC-19. Many safeguards for mobile devices are reflected in other controls. AC-20 addresses mobile devices that are not organization-controlled.

Related Controls: AC-3, AC-4, AC-7, AC-11, AC-17, AC-18, AC-20, CA-9, CM-2, CM-6, IA-2, IA-3, MP-2, MP-4, MP-5, MP-7, PL-4, SC-7, SC-34, SC-43, SI-3, SI-4.

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*].

Discussion: None.

Related Controls: CM-8, IR-4.

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

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

Discussion: Container-based encryption provides a more fine-grained approach to data and information encryption on mobile devices, including encrypting selected data structures such as files, records, or fields.

Related Controls: SC-12, SC-13, SC-28.

References: [SP 800-114], [SP 800-124].

AC-20 USE OF EXTERNAL SYSTEMS

Control:

a. [*Selection (one or more): Establish* [*Assignment: organization-defined terms and conditions*]*; Identify* [*Assignment: organization-defined controls asserted to be implemented on external systems*]], consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to:

   1. Access the system from external systems; and

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

b. Prohibit the use of [*Assignment: organizationally-defined types of external systems*].

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

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

External systems used to access public interfaces to organizational systems are outside the scope of AC-20. Organizations establish specific terms and conditions for the use of external systems in accordance with organizational security policies and procedures. At a minimum, terms and conditions address the specific types of applications that can be accessed on organizational

systems from external systems and the highest security category of information that can be processed, stored, or transmitted on external systems. If the terms and conditions with the owners of the external systems cannot be established, organizations may impose restrictions on organizational personnel using those external systems.

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

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

Discussion: Limiting authorized use recognizes circumstances where individuals using external systems may need to access organizational systems. Organizations need assurance that the external systems contain the necessary controls so as not to compromise, damage, or otherwise harm organizational systems. Verification that the required controls have been implemented can be achieved by external, independent assessments, attestations, or other means, depending on the confidence level required by organizations.

Related Controls: CA-2.

(2) USE OF EXTERNAL SYSTEMS | PORTABLE STORAGE DEVICES — RESTRICTED USE

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

Discussion: Limits on the use of organization-controlled portable storage devices in external systems include restrictions on how the devices may be used and under what conditions the devices may be used.

Related Controls: MP-7, SC-41.

(3) USE OF EXTERNAL SYSTEMS | NON-ORGANIZATIONALLY OWNED SYSTEMS — RESTRICTED USE

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

Discussion: Non-organizationally owned systems or system components include systems or system components owned by other organizations as well as personally owned devices. There are potential risks to using non-organizationally owned systems or components. In some cases, the risk is sufficiently high as to prohibit such use (see AC-20 b.). In other cases, the use of such systems or system components may be allowed but restricted in some way. Restrictions include requiring the implementation of approved controls prior to authorizing the connection of non-organizationally owned systems and components; limiting access to types of information, services, or applications; using virtualization techniques to limit processing and storage activities to servers or system components provisioned by the organization; and agreeing to the terms and conditions for usage. Organizations consult with the Office of the General Counsel regarding legal issues associated with using personally owned devices, including requirements for conducting forensic analyses during investigations after an incident.

Related Controls: None.

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

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

Discussion: Network-accessible storage devices in external systems include online storage devices in public, hybrid, or community cloud-based systems.

Related Controls: None.

(5) USE OF EXTERNAL SYSTEMS | PORTABLE STORAGE DEVICES — PROHIBITED USE

Prohibit the use of organization-controlled portable storage devices by authorized individuals on external systems.

Discussion: Limits on the use of organization-controlled portable storage devices in external systems include a complete prohibition of the use of such devices. Prohibiting such use is enforced using technical methods and/or nontechnical (i.e., process-based) methods.

Related Controls: MP-7, PL-4, PS-6, SC-41.

References: [FIPS 199], [SP 800-171], [SP 800-172].

AC-21 INFORMATION SHARING

Control:

a. Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions for [*Assignment: organization-defined information sharing circumstances where user discretion is required*]; and

b. Employ [*Assignment: organization-defined automated mechanisms or manual processes*] to assist users in making information sharing and collaboration decisions.

Discussion: Information sharing applies to information that may be restricted in some manner based on some formal or administrative determination. Examples of such information include, contract-sensitive information, classified information related to special access programs or compartments, privileged information, proprietary information, and personally identifiable information. Security and privacy risk assessments as well as applicable laws, regulations, and policies can provide useful inputs to these determinations. Depending on the circumstances, sharing partners may be defined at the individual, group, or organizational level. Information may be defined by content, type, security category, or special access program or compartment. Access restrictions may include non-disclosure agreements (NDA). Information flow techniques and security attributes may be used to provide automated assistance to users making sharing and collaboration decisions.

Related Controls: AC-3, AC-4, AC-16, PT-2, PT-7, RA-3, SC-15.

Control Enhancements:

(1) INFORMATION SHARING | AUTOMATED DECISION SUPPORT

Employ [*Assignment: organization-defined automated mechanisms]* to enforce information-sharing decisions by authorized users based on access authorizations of sharing partners and access restrictions on information to be shared.

Discussion: Automated mechanisms are used to enforce information sharing decisions.

Related Controls: None.

(2) INFORMATION SHARING | INFORMATION SEARCH AND RETRIEVAL

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

Discussion: Information search and retrieval services identify information system resources relevant to an information need.

Related Controls: None.

References: [OMB A-130], [SP 800-150], [IR 8062].

AC-22 PUBLICLY ACCESSIBLE CONTENT

Control:

a. Designate individuals authorized to make information publicly accessible;

b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information;

c. Review the proposed content of information prior to posting onto the publicly accessible system to ensure that nonpublic information is not included; and

d. Review the content on the publicly accessible system for nonpublic information [*Assignment: organization-defined frequency*] and remove such information, if discovered.

Discussion: In accordance with applicable laws, executive orders, directives, policies, regulations, standards, and guidelines, the public is not authorized to have access to nonpublic information, including information protected under the [PRIVACT] and proprietary information. Publicly accessible content addresses systems that are controlled by the organization and accessible to the public, typically without identification or authentication. Posting information on non-organizational systems (e.g., non-organizational public websites, forums, and social media) is covered by organizational policy. While organizations may have individuals who are responsible for developing and implementing policies about the information that can be made publicly accessible, publicly accessible content addresses the management of the individuals who make such information publicly accessible.

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

Control Enhancements: None.

References: [PRIVACT].

AC-23 DATA MINING PROTECTION

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

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

Data mining prevention and detection techniques include limiting the number and frequency of database queries to increase the work factor needed to determine the contents of databases, limiting types of responses provided to database queries, applying differential privacy techniques or homomorphic encryption, and notifying personnel when atypical database queries or accesses occur. Data mining protection focuses on protecting information from data mining while such information resides in organizational data stores. In contrast, AU-13 focuses on monitoring for organizational information that may have been mined or otherwise obtained from data stores

and is available as open-source information residing on external sites, such as social networking or social media websites.

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

Related Controls: PM-12, PT-2.

Control Enhancements: None.

References: [EO 13587].

AC-24 ACCESS CONTROL DECISIONS

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

Discussion: Access control decisions (also known as authorization decisions) occur when authorization information is applied to specific accesses. In contrast, access enforcement occurs when systems enforce access control decisions. While it is common to have access control decisions and access enforcement implemented by the same entity, it is not required, and it is not always an optimal implementation choice. For some architectures and distributed systems, different entities may make access control decisions and enforce access.

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 controls*] to [*Assignment: organization-defined systems*] that enforce access control decisions.

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

Related Controls: AU-10.

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

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

Discussion: In certain situations, it is important that access control decisions can be made without information regarding the identity of the users issuing the requests. These are generally instances where preserving individual privacy is of paramount importance. In other

situations, user identification information is simply not needed for access control decisions, and especially in the case of distributed systems, transmitting such information with the needed degree of assurance may be very expensive or difficult to accomplish. MAC, RBAC, ABAC, and label-based control policies, for example, might not include user identity as an attribute.

Related Controls: None.

References: [SP 800-162], [SP 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.

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

Related Controls: AC-3, AC-16, SA-8, SA-17, SC-3, SC-11, SC-39, SI-13.

Control Enhancements: None.

References: None.