NIST SP800-53
ACCESS CONTROL

ACCESS CONTROL POLICY AND PROCEDURES

organization-defined personnel or roles
organization-defined personnel or roles

organization-defined senior management official
organization-defined senior management official

organization-defined frequency
organization-defined frequency

organization-defined frequency
organization-defined frequency
name: AC-1

statement

item
name: AC-1a.

Develop, document, and disseminate to :

item
name: AC-1a.1.

An access control policy that:

item
name: AC-1a.1.(a)

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

item
name: AC-1a.1.(b)

Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and

item
name: AC-1a.2.

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

item
name: AC-1b.

Designate an to manage the access control policy and procedures;

item
name: AC-1c.

Review and update the current access control:

item
name: AC-1c.1.

Policy ; and

item
name: AC-1c.2.

Procedures ;

item
name: AC-1d.

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

item
name: AC-1e.

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

guidance

This control addresses the establishment of policy and procedures for the effective implementation of the controls and control enhancements in the AC family. The risk management strategy is an important factor in establishing policy and procedures. Comprehensive policy and procedures help provide security and privacy assurance. Security and privacy program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general security and privacy policy or can be represented by multiple policies reflecting the complex nature of organizations. The procedures can be established for security and privacy programs and for systems, if needed. Procedures describe how policies or controls are implemented and can be directed at the personnel or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. It is

important to recognize that restating controls does not constitute an organizational policy or procedure.

References

NIST Special Publication 800-12
NIST Special Publication 800-30
NIST Special Publication 800-39
NIST Special Publication 800-100

ACCOUNT MANAGEMENT

organization-defined personnel or roles
organization-defined personnel or roles

organization-defined policy, procedures, and conditions
organization-defined policy, procedures, and conditions

organization-defined time-period for each situation
organization-defined time-period for each situation

organization-defined frequency
organization-defined frequency
name: AC-2

statement

item
name: AC-2a.

Define and document the types of system accounts allowed for use within the system in support of organizational missions and business functions;

item
name: AC-2b.

Assign account managers for system accounts;

item
name: AC-2c.

Establish conditions for group and role membership;

item
name: AC-2d.

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

item
name: AC-2e.

Require approvals by for requests to create system accounts;

item
name: AC-2f.

Create, enable, modify, disable, and remove system accounts in accordance with ;

item
name: AC-2g.

Monitor the use of system accounts;

item
name: AC-2h.

Notify account managers within :

item
name: AC-2h.1.

When accounts are no longer required;

item
name: AC-2h.2.

When users are terminated or transferred; and

item
name: AC-2h.3.

When individual system usage or need-to-know changes for an individual;

item
name: AC-2i.

Authorize access to the system based on:

item
name: AC-2i.1.

A valid access authorization;

item
name: AC-2i.2.

Intended system usage; and

item
name: AC-2i.3.

Other attributes as required by the organization or associated missions and business functions;

item
name: AC-2j.

Review accounts for compliance with account management requirements ;

item
name: AC-2k.

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

item
name: AC-2l.

Align account management processes with personnel termination and transfer processes.

guidance

System account types include, for example, individual, shared, group, system, guest, anonymous, emergency, developer/manufacturer/vendor, temporary, and service. The identification of authorized users of the system and the specification of access privileges reflects the requirements in other controls in the security plan. Users requiring administrative privileges on system accounts receive additional scrutiny by appropriate organizational personnel responsible for approving such accounts and privileged access, including, for example, system owner, mission/ business owner, or chief information security officer. Organizations may choose to define access privileges or other attributes by account, by type of account, or a combination of both. Other attributes required for authorizing access include, for example, restrictions on time-of-day, day-of-week, and point-of-origin. In defining other account attributes, organizations consider system-related requirements 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 a part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation. Organizations establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes. Emergency and temporary accounts are not to be confused with infrequently used accounts including, for example, local logon accounts used for special tasks or when network resources are unavailable. Such accounts remain available and are not subject to automatic disabling or removal dates. Conditions for disabling or deactivating accounts include, for example, when shared/group, emergency, or temporary accounts are no longer required; or when individuals are transferred or terminated. Some types of system accounts may require specialized training.

AUTOMATED SYSTEM ACCOUNT MANAGEMENT

name: AC-2 (1)

statement

Employ automated mechanisms to support the management of system accounts.

guidance

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

None

REMOVAL OF TEMPORARY AND EMERGENCY ACCOUNTS

organization-defined time-period for each type of account
organization-defined time-period for each type of account

name: AC-2 (2)

statement

Automatically [Selection: remove; disable] temporary and emergency accounts after .

guidance

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

None

DISABLE ACCOUNTS

organization-defined time-period
organization-defined time-period

name: AC-2 (3)

statement

Automatically disable accounts when the accounts:

item

name: AC-2 (3)(a)

Have expired;

item

name: AC-2 (3)(b)

Are no longer associated to a user;

item
name: AC-2 (3)(c)

Are in violation of organizational policy;

item
name: AC-2 (3)(d)

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

item
name: AC-2 (3)(e)

Have been inactive for .

guidance

None.
None

AUTOMATED AUDIT ACTIONS

organization-defined personnel or roles
organization-defined personnel or roles
name: AC-2 (4)

statement

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

guidance

None.

INACTIVITY LOGOUT

organization-defined time-period of expected inactivity or description of when to log out
organization-defined time-period of expected inactivity or description of when to log out
name: AC-2 (5)

statement

Require that users log out when .

guidance

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

DYNAMIC PRIVILEGE MANAGEMENT

organization-defined list of dynamic privilege management capabilities
organization-defined list of dynamic privilege management capabilities
name: AC-2 (6)

statement

Implement the following dynamic privilege management capabilities: .

guidance

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

ROLE-BASED SCHEMES

name: AC-2 (7)

statement

item
name: AC-2 (7)(a)

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

item
name: AC-2 (7)(b)

Monitor privileged role assignments; and

item
name: AC-2 (7)(c)

Revoke access when privileged role assignments are no longer appropriate.

guidance

Privileged roles are organization-defined roles assigned to individuals that allow those individuals to perform certain security-relevant functions that ordinary users are not authorized to perform. These privileged roles include, for example, key management, account management, network and system administration, database administration, and web administration.
None

DYNAMIC ACCOUNT MANAGEMENT

organization-defined system accounts
organization-defined system accounts
name: AC-2 (8)

statement

Create, activate, manage, and deactivate dynamically.

guidance

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

RESTRICTIONS ON USE OF SHARED AND GROUP ACCOUNTS

organization-defined conditions for establishing shared and group accounts
organization-defined conditions for establishing shared and group accounts
name: AC-2 (9)

statement

Only permit the use of shared and group accounts that meet .

guidance

Before permitting the use of shared or group accounts, organizations consider the increased risk due to the lack of accountability with such accounts.
None

SHARED AND GROUP ACCOUNT CREDENTIAL CHANGE

name: AC-2 (10)

statement

Change shared and group account credentials when members leave the group.

guidance

This control enhancement is intended to ensure that former group members do not retain access to the shared/group account.
None

USAGE CONDITIONS

organization-defined circumstances and/or usage conditions
organization-defined circumstances and/or usage conditions

organization-defined system accounts
organization-defined system accounts
name: AC-2 (11)

statement

Enforce for .

guidance

This control enhancement helps to enforce the principle of least privilege, increase user accountability, and enable more effective account monitoring. Such monitoring includes, for example, alerts generated if the account is used outside of specified parameters. Organizations can describe the specific conditions or circumstances under which system accounts can be used, for example, by restricting usage to certain days of the week, time of day, or specific durations of time.
None

ACCOUNT MONITORING FOR ATYPICAL USAGE

organization-defined atypical usage
organization-defined atypical usage

organization-defined personnel or roles
organization-defined personnel or roles
name: AC-2 (12)

statement

item
name: AC-2 (12)(a)

Monitor system accounts for ; and

item

name: AC-2 (12)(b)

Report atypical usage of system accounts to .

guidance

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

DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS

organization-defined time-period
organization-defined time-period
name: AC-2 (13)

statement

Disable accounts of users posing a significant risk within of discovery of the risk.

guidance

Users posing a significant risk to organizations include individuals for whom reliable evidence or intelligence indicates either the intention to use authorized access to systems to cause harm or through whom adversaries will cause harm. Such harm includes the potential adverse impacts to organizational operations and assets, individuals, other organizations, or the Nation. Close coordination and cooperation among authorizing officials, system administrators, and human resource managers is essential for timely execution of this control enhancement.

PROHIBIT SPECIFIC ACCOUNT TYPES

organization-defined information types
organization-defined information types
name: AC-2 (14)

statement

Prohibit the creation and use of [Selection (one or more): shared; guest; anonymous; temporary; emergency] accounts for access to .

guidance

NIST Special Publications 800-162, 800-178.

ATTRIBUTE-BASED SCHEMES

name: AC-2 (15)

statement

item
name: AC-2 (15)(a)

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

item
name: AC-2 (15)(b)

Monitor privileged attribute-based assignments;

item
name: AC-2 (15)(c)

Monitor changes to attributes; and

item
name: AC-2 (15)(d)

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

guidance

Privileged roles are organization-defined roles assigned to individuals that allow those individuals to perform certain security-relevant functions that ordinary users are not authorized to perform. These privileged roles include, for example, key management, account management, network and system administration, database administration, and web administration.
None

ACCESS ENFORCEMENT
name: AC-3

statement

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

guidance

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 organizational missions and business operations, access enforcement mechanisms can also be employed at the application and service level to provide increased information security.

MA-5 MP-4

RESTRICTED ACCESS TO PRIVILEGED FUNCTIONS

name: AC-3 (1)

statement

Incorporated into AC-6.

DUAL AUTHORIZATION

organization-defined privileged commands and/or other organization-defined actions
organization-defined privileged commands and/or other organization-defined actions
name: AC-3 (2)

statement

Enforce dual authorization for .

guidance

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

MANDATORY ACCESS CONTROL

organization-defined mandatory access control policy
organization-defined mandatory access control policy

organization-defined subjects
organization-defined subjects

organization-defined privileges
organization-defined privileges
name: AC-3 (3)

statement

Enforce over all subjects and objects where the policy:

item
name: AC-3 (3)(a)

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

item
name: AC-3 (3)(b)

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

item
name: AC-3 (3)(b)(1)

Passing the information to unauthorized subjects or objects;

item
name: AC-3 (3)(b)(2)

Granting its privileges to other subjects;

item
name: AC-3 (3)(b)(3)

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

item
name: AC-3 (3)(b)(4)

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

item
name: AC-3 (3)(b)(5)

Changing the rules governing access control; and

item
name: AC-3 (3)(c)

Specifies that may explicitly be granted such that they are not limited by any of the above constraints.

guidance

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

the constraints on the information remain in effect). The trusted subjects described above are granted privileges consistent with the concept of least privilege (see AC-6). Trusted subjects are only given the minimum privileges relative to the above policy necessary for satisfying organizational mission/business needs. The control is most applicable when there is a policy mandate 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. This control can operate in conjunction with AC-3(4). A subject constrained in its operation by policies governed by this control is still able to operate under the less rigorous constraints of AC-3(4), but policies governed by this control take precedence over the less rigorous constraints of AC-3(4). For example, while a mandatory access control policy imposes a constraint preventing a subject from passing information to another subject operating at a different sensitivity label, AC-3(4) permits the subject to pass the information to any subject with the same sensitivity label as the subject.

DISCRETIONARY ACCESS CONTROL

organization-defined discretionary access control policy
organization-defined discretionary access control policy
name: AC-3 (4)

statement

Enforce over defined subjects and objects where the policy specifies that a subject that has been granted access to information can do one or more of the following:

item
name: AC-3 (4)(a)

Pass the information to any other subjects or objects;

item
name: AC-3 (4)(b)

Grant its privileges to other subjects;

item
name: AC-3 (4)(c)

Change security attributes on subjects, objects, the system, or the system#s components;

item
name: AC-3 (4)(d)

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

item
name: AC-3 (4)(e)

Change the rules governing access control.

guidance

When discretionary access control policies are implemented, subjects are not constrained regarding what actions they can take with information for which they have already been granted access. Thus, subjects that have been granted access to information are not prevented from passing (i.e., the subjects have the discretion to pass) the information to other subjects or objects. This control enhancement can operate in conjunction with AC-3(3). A subject that is constrained in its operation by policies governed by AC-3(3) is still able to operate under the less rigorous constraints of this control enhancement. Therefore, while AC-3(3) imposes constraints preventing a subject from passing information to another subject operating at a different sensitivity level, AC-3(4) permits the subject to pass the information to any subject at the same sensitivity level. The policy is bounded by the system boundary. Once the information is passed outside of the control of the system, additional means may be required to help ensure that the constraints remain in effect. While the older, more traditional definitions of discretionary access control require identity-based access control, that limitation is not required for this use of discretionary access control.
None

SECURITY-RELEVANT INFORMATION

organization-defined security-relevant information
organization-defined security-relevant information
name: AC-3 (5)

statement

Prevent access to except during secure, non-operable system states.

guidance

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

PROTECTION OF USER AND SYSTEM INFORMATION

name: AC-3 (6)

statement

Incorporated into MP-4 and SC-28.

ROLE-BASED ACCESS CONTROL

organization-defined roles and users authorized to assume such roles
organization-defined roles and users authorized to assume such roles
name: AC-3 (7)

statement

Enforce a role-based access control policy over defined subjects and objects and control access based upon .

guidance

Role-based access control (RBAC) is an access control policy that restricts system access to authorized users. Organizations can create specific roles based on job functions and the authorizations (i.e., privileges) to perform needed operations on the systems associated with the organization-defined roles. When users are assigned to the organizational roles, they inherit the authorizations or privileges defined for those roles. RBAC simplifies privilege administration for organizations because privileges are not assigned directly to every user (which can be a significant number of individuals for mid- to large-size organizations) but are instead acquired through role assignments. RBAC can be implemented either as a mandatory or discretionary form of access control. For organizations implementing RBAC with mandatory access controls, the requirements in AC-3(3) define the scope of the subjects and objects covered by the policy.

REVOCATION OF ACCESS AUTHORIZATIONS

organization-defined rules governing the timing of revocations of access authorizations
organization-defined rules governing the timing of revocations of access authorizations
name: AC-3 (8)

statement

Enforce the revocation of access authorizations resulting from changes to the security attributes of subjects and objects based on .

guidance

Revocation of access rules may differ based on the types of access revoked. For example, if a subject (i.e., user or process) is removed from a group, access may not be revoked until the next time the object is opened or the next time the subject attempts a new access to the object. Revocation based on changes to security labels may take effect immediately. Organizations provide alternative approaches on how to make revocations immediate if systems cannot provide such capability and immediate revocation is necessary.
None

CONTROLLED RELEASE

organization-defined system or system component
organization-defined system or system component

organization-defined security safeguards
organization-defined security safeguards

organization-defined security safeguards
organization-defined security safeguards
name: AC-3 (9)

statement

Release information outside of the established system boundary only if:

item
name: AC-3 (9)(a)

The receiving provides ; and

item
name: AC-3 (9)(b)

are used to validate the appropriateness of the information designated for release.

guidance

Systems can only protect organizational information within the confines of established system boundaries. Additional security controls may be needed to ensure that such information is adequately protected once it is passed beyond the established system boundaries. In situations where the system is unable to determine the adequacy of the protections provided by entities outside its boundary, as a mitigating control, organizations determine procedurally whether the external systems are providing adequate security. The means used to determine the adequacy of security provided by external systems include, for example, conducting inspections or periodic testing and assessments; establishing agreements between the organization and its counterpart organizations; or some other process. The means used by external entities to protect the information received need not be the same as those used by the organization, but the means employed are sufficient to provide consistent adjudication of the security policy to protect the information. This control enhancement requires systems to employ technical or procedural means to validate the information prior to releasing it to external systems. For example, if the system passes information to another system controlled by another organization, technical means are employed to validate that the security attributes associated with the exported information are appropriate for the receiving system. Alternatively, if the system passes information to a printer in organization-controlled space, procedural means can be employed to ensure that only appropriately authorized individuals gain access to the printer. This control enhancement is most

applicable when there is some policy mandate that establishes policy regarding access to the information, and that policy applies beyond the realm of a particular system or organization.

AUDITED OVERRIDE OF ACCESS CONTROL MECHANISMS

organization-defined conditions
organization-defined conditions

organization-defined roles
organization-defined roles
name: AC-3 (10)

statement

Employ an audited override of automated access control mechanisms under by .

guidance

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

RESTRICT ACCESS TO SPECIFIC INFORMATION

organization-defined information types
organization-defined information types
name: AC-3 (11)

statement

Restrict direct access to data repositories containing .

guidance

This control enhancement is intended to provide flexibility regarding access control of specific pieces of information within a system. For example, role-based access could be employed to allow access to only a specific type of personally identifiable information within a database rather than allowing access to the database in its entirety.
None

ASSERT AND ENFORCE APPLICATION ACCESS

organization-defined system applications and functions
organization-defined system applications and functions
name: AC-3 (12)

statement

item
name: AC-3 (12)(a)

Require applications to assert, as part of the installation process, the access needed to the following system applications and functions: ; and

item
name: AC-3 (12)(b)

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

guidance

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

ATTRIBUTE-BASED ACCESS CONTROL

organization-defined attributes to assume access permissions
organization-defined attributes to assume access permissions
name: AC-3 (13)

statement

Enforce attribute-based access control policy over defined subjects and objects and control access based upon .

guidance

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

INFORMATION FLOW ENFORCEMENT

organization-defined information flow control policies
organization-defined information flow control policies
name: AC-4

statement

Enforce approved authorizations for controlling the flow of information within the system and between interconnected systems based on .

guidance

Information flow control regulates where information can travel within a system and between systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. Flow control restrictions include, for example, keeping export-controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization, restricting web requests to the Internet that are not from the internal web proxy server, and limiting information transfers between organizations based on data structures and content. Transferring information between systems in different security domains with different security policies introduces risk that such transfers violate one or more domain security policies. In such situations, information owners or stewards provide guidance at designated policy enforcement points between interconnected systems. Organizations consider mandating specific architectural solutions when required to enforce specific security policies. Enforcement includes, for example, prohibiting information transfers between interconnected systems (i.e., allowing access only); employing hardware mechanisms to enforce one-way information flows; and implementing trustworthy regrading mechanisms to reassign security attributes and security labels. Organizations commonly employ information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations within systems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Enforcement occurs, for example, in boundary protection devices that employ rule sets or establish configuration settings that restrict system services, provide a packet-filtering capability based on header information, or message-filtering capability based on message content. Organizations also consider the trustworthiness of filtering/inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement. Control enhancements 3 through 22 primarily address cross-domain solution needs which focus on more advanced filtering techniques, in-depth analysis, and stronger flow enforcement mechanisms implemented in cross-domain products, for example, high-assurance guards. Such capabilities are generally not available in commercial off-the-shelf information technology products.

OBJECT SECURITY ATTRIBUTES

organization-defined security attributes
organization-defined security attributes

organization-defined information, source, and destination objects
organization-defined information, source, and destination objects

organization-defined information flow control policies

organization-defined information flow control policies
name: AC-4 (1)

statement

Use associated with to enforce as a basis for flow control decisions.

guidance

Information flow enforcement mechanisms compare security attributes associated with information (data content and data structure) and source/destination objects, and respond appropriately when the mechanisms encounter information flows not explicitly allowed by information flow policies. For example, an information object labeled Secret would be allowed to flow to a destination object labeled Secret, but an information object labeled Top Secret would not be allowed to flow to a destination object labeled Secret. Security attributes can also include, for example, source and destination addresses employed in traffic filter firewalls. Flow enforcement using explicit security attributes can be used, for example, to control the release of certain types of information.
None

PROCESSING DOMAINS

organization-defined information flow control policies
organization-defined information flow control policies
name: AC-4 (2)

statement

Use protected processing domains to enforce as a basis for flow control decisions.

guidance

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

DYNAMIC INFORMATION FLOW CONTROL

organization-defined policies
organization-defined policies
name: AC-4 (3)

statement

Enforce dynamic information flow control based on .

guidance

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

FLOW CONTROL OF ENCRYPTED INFORMATION

organization-defined flow control mechanisms
organization-defined flow control mechanisms

organization-defined procedure or method
organization-defined procedure or method
name: AC-4 (4)

statement

Prevent encrypted information from bypassing by [Selection (one or more): decrypting the information; blocking the flow of the encrypted information; terminating communications sessions attempting to pass encrypted information;].

guidance

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

EMBEDDED DATA TYPES

organization-defined limitations
organization-defined limitations
name: AC-4 (5)

statement

Enforce on embedding data types within other data types.

guidance

Embedding data types within other data types may result in reduced flow control effectiveness. Data type embedding includes, for example, inserting executable files as objects within word processing files, inserting references or descriptive information into a media file, and compressed or archived data types that may include multiple embedded data types. Limitations on data type embedding consider the levels of embedding and prohibit levels of data type embedding that are beyond the capability of the inspection tools.

None

METADATA

organization-defined metadata
organization-defined metadata
name: AC-4 (6)

statement

Enforce information flow control based on .

guidance

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

ONE-WAY FLOW MECHANISMS

organization-defined one-way information flows
organization-defined one-way information flows
name: AC-4 (7)

statement

Enforce using hardware mechanisms.

guidance

None.
None

SECURITY POLICY FILTERS

organization-defined security policy filters
organization-defined security policy filters

organization-defined information flows
organization-defined information flows
name: AC-4 (8)

statement

Enforce information flow control using as a basis for flow control decisions for .

guidance

Organization-defined security policy filters can address data structures and content. For example, security policy filters for data structures can check for maximum file lengths, maximum field sizes, and data/file types (for structured and unstructured data). Security policy filters for data content can check for specific words 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 sensitivity 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 policy filter to meet information flow control objectives.
None

HUMAN REVIEWS

organization-defined information flows
organization-defined information flows

organization-defined conditions
organization-defined conditions
name: AC-4 (9)

statement

Enforce the use of human reviews for under the following conditions: .

guidance

Organizations define security policy filters for all situations where automated flow control decisions are possible. When a fully automated flow control decision is not possible, then a human review may be employed in lieu of, or as a complement to, automated security policy filtering. Human reviews may also be employed as deemed necessary by organizations.
None

ENABLE AND DISABLE SECURITY POLICY FILTERS

organization-defined security policy filters
organization-defined security policy filters

organization-defined conditions
organization-defined conditions
name: AC-4 (10)

statement

Provide the capability for privileged administrators to enable and disable under the following conditions: .

guidance

For example, as allowed by the system authorization, administrators can enable security policy filters to accommodate approved data types.
None

CONFIGURATION OF SECURITY POLICY FILTERS

organization-defined security policy filters
organization-defined security policy filters
name: AC-4 (11)

statement

Provide the capability for privileged administrators to configure to support different security policies.

guidance

For example, to reflect changes in security policies, administrators can change the list of #dirty words# that security policy mechanisms check in accordance with the definitions provided by organizations.
None

DATA TYPE IDENTIFIERS

organization-defined data type identifiers
organization-defined data type identifiers
name: AC-4 (12)

statement

When transferring information between different security domains, use to validate data essential for information flow decisions.

guidance

Data type identifiers include, for example, filenames, file types, file signatures/tokens, and multiple internal file signatures/tokens. Systems may allow transfer of data only if compliant with data type format specifications.
None

DECOMPOSITION INTO POLICY-RELEVANT SUBCOMPONENTS

organization-defined policy-relevant subcomponents
organization-defined policy-relevant subcomponents
name: AC-4 (13)

statement

When transferring information between different security domains, decompose information into for submission to policy enforcement mechanisms.

guidance

Policy enforcement mechanisms apply filtering, inspection, and/or sanitization rules to the policy-relevant subcomponents of information to facilitate flow enforcement prior to transferring such information to different security domains. Parsing transfer files facilitates policy decisions on source, destination, certificates, classification, attachments, and other security-related component differentiators.
None

SECURITY POLICY FILTER CONSTRAINTS

organization-defined security policy filters
organization-defined security policy filters
name: AC-4 (14)

statement

When transferring information between different security domains, implement requiring fully enumerated formats that restrict data structure and content.

guidance

Data structure and content restrictions reduce the range of potential malicious or unsanctioned content in cross-domain transactions. Security policy filters that restrict data structures include, for example, restricting file sizes and field lengths. Data content policy filters include, for example, encoding formats for character sets; restricting character data fields to only contain alpha-numeric characters; prohibiting special characters; and validating schema structures.
None

DETECTION OF UNSANCTIONED INFORMATION

organized-defined unsanctioned information
organized-defined unsanctioned information

organization-defined security policy

organization-defined security policy
name: AC-4 (15)

statement

When transferring information between different security domains, examine the information for the presence of and prohibit the transfer of such information in accordance with the .

guidance

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

INFORMATION TRANSFERS ON INTERCONNECTED SYSTEMS

name: AC-4 (16)

statement

Incorporated into AC-4.

DOMAIN AUTHENTICATION

name: AC-4 (17)

statement

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

guidance

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

SECURITY ATTRIBUTE BINDING

name: AC-4 (18)

statement

Incorporated into AC-16.

VALIDATION OF METADATA

name: AC-4 (19)

statement

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

guidance

This control enhancement requires the validation of metadata and the data to which the metadata applies. Some organizations distinguish between metadata and data payloads (i.e., only the data to which the metadata is bound). Other organizations do not make such distinctions, considering metadata and the data to which the metadata applies as part of the payload. All information (including metadata and the data to which the metadata applies) is subject to filtering and inspection.
None

APPROVED SOLUTIONS

organization-defined solutions in approved configurations
organization-defined solutions in approved configurations

organization-defined information
organization-defined information
name: AC-4 (20)

statement

Employ to control the flow of across security domains.

guidance

Organizations define approved solutions and configurations in cross-domain policies and guidance in accordance with the types of information flows across classification boundaries. The Unified Cross Domain Management Office provides a baseline listing of approved cross-domain solutions.
None

PHYSICAL AND LOGICAL SEPARATION OF INFORMATION FLOWS

organization-defined mechanisms and/or techniques
organization-defined mechanisms and/or techniques

organization-defined required separations by types of information
organization-defined required separations by types of information
name: AC-4 (21)

statement

Separate information flows logically or physically using to accomplish .

guidance

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

ACCESS ONLY

name: AC-4 (22)

statement

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

guidance

The system, for example, provides a desktop for users to access each connected security domain without providing any mechanisms to allow transfer of information between the different security domains.
None

SEPARATION OF DUTIES

organization-defined duties of individuals
organization-defined duties of individuals
name: AC-5

statement

item
name: AC-5a.

Separate ;

item
name: AC-5b.

Document separation of duties of individuals; and

item
name: AC-5c.

Define system access authorizations to support separation of duties.

guidance

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

LEAST PRIVILEGE

name: AC-6

statement

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

guidance

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

AUTHORIZE ACCESS TO SECURITY FUNCTIONS

organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information

organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information

name: AC-6 (1)

statement

Explicitly authorize access to .

guidance

Security functions include, for example, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and establishing intrusion detection parameters. Security-relevant information includes, for example, filtering

rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists. Explicitly authorized personnel include, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users.

NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS

organization-defined security functions or security-relevant information
organization-defined security functions or security-relevant information
name: AC-6 (2)

statement

Require that users of system accounts, or roles, with access to , use non-privileged accounts or roles, when accessing nonsecurity functions.

guidance

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

NETWORK ACCESS TO PRIVILEGED COMMANDS

organization-defined privileged commands
organization-defined privileged commands

organization-defined compelling operational needs
organization-defined compelling operational needs
name: AC-6 (3)

statement

Authorize network access to only for and document the rationale for such access in the security plan for the system.

guidance

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

SEPARATE PROCESSING DOMAINS

name: AC-6 (4)

statement

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

guidance

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

PRIVILEGED ACCOUNTS

organization-defined personnel or roles
organization-defined personnel or roles
name: AC-6 (5)

statement

Restrict privileged accounts on the system to .

guidance

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

PRIVILEGED ACCESS BY NON-ORGANIZATIONAL USERS

name: AC-6 (6)

statement

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

guidance

None.

REVIEW OF USER PRIVILEGES

organization-defined frequency
organization-defined frequency

organization-defined roles or classes of users
organization-defined roles or classes of users
name: AC-6 (7)

statement

item
name: AC-6 (7)(a)

Review the privileges assigned to to validate the need for such privileges; and

item
name: AC-6 (7)(b)

Reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs.

guidance

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

PRIVILEGE LEVELS FOR CODE EXECUTION

organization-defined software
organization-defined software
name: AC-6 (8)

statement

Prevent the following software from executing at higher privilege levels than users executing the software: .

guidance

In certain situations, software applications/programs need to execute with elevated privileges to perform required functions. However, if the privileges required for execution are at a higher level than the privileges assigned to organizational users invoking such applications/programs, those users are indirectly provided with greater privileges than assigned by organizations.
None

AUDITING USE OF PRIVILEGED FUNCTIONS

name: AC-6 (9)

statement

Audit the execution of privileged functions.

guidance

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

PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS

name: AC-6 (10)

statement

Prevent non-privileged users from executing privileged functions.

guidance

Privileged functions include, for example, disabling, circumventing, or altering implemented security or privacy controls, establishing system accounts, performing system integrity checks, or administering cryptographic key management activities. Non-privileged users are individuals that do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users.
None

UNSUCCESSFUL LOGON ATTEMPTS

organization-defined number
organization-defined number

organization-defined time-period
organization-defined time-period

organization-defined time-period
organization-defined time-period

organization-defined delay algorithm
organization-defined delay algorithm

organization-defined action
organization-defined action

name: AC-7

statement

item
name: AC-7a.

Enforce a limit of consecutive invalid logon attempts by a user during a ; and

item
name: AC-7b.

Automatically [Selection (one or more): lock the account/node for an ; lock the account/node until released by an administrator; delay next logon prompt per ; take] when the maximum number of unsuccessful attempts is exceeded.

guidance

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

AUTOMATIC ACCOUNT LOCK

name: AC-7 (1)

statement

Incorporated into AC-7.

PURGE OR WIPE MOBILE DEVICE

organization-defined mobile devices
organization-defined mobile devices

organization-defined purging or wiping requirements and techniques
organization-defined purging or wiping requirements and techniques

organization-defined number
organization-defined number
name: AC-7 (2)

statement

Purge or wipe information from based on after consecutive, unsuccessful device logon attempts.

guidance

This control enhancement applies only to mobile devices for which a logon 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.

BIOMETRIC ATTEMPT LIMITING

organization-defined number
organization-defined number
name: AC-7 (3)

statement

Limit the number of unsuccessful biometric logon attempts to .

guidance

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

USE OF ALTERNATE FACTOR

name: AC-7 (4)

statement

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

guidance

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

References

NIST Special Publication 800-63
NIST Special Publication 800-124

SYSTEM USE NOTIFICATION

organization-defined system use notification message or banner
organization-defined system use notification message or banner

organization-defined conditions
organization-defined conditions
name: AC-8

statement

item
name: AC-8a.

Display to users before granting access to the system that provides privacy and security notices consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidelines and state that:

item
name: AC-8a.1.

Users are accessing a U.S. Government system;

item
name: AC-8a.2.

System usage may be monitored, recorded, and subject to audit;

item
name: AC-8a.3.

Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and

item
name: AC-8a.4.

Use of the system indicates consent to monitoring and recording;

item
name: AC-8b.

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

item
name: AC-8c.

For publicly accessible systems:

item
name: AC-8c.1.

Display system use information , before granting further access to the publicly accessible system;

item
name: AC-8c.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

item
name: AC-8c.3.

Include a description of the authorized uses of the system.

guidance

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

PREVIOUS LOGON (ACCESS) NOTIFICATION
name: AC-9

statement

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

guidance

This control is applicable to logons to systems via human user interfaces and logons to systems that occur in other types of architectures.

UNSUCCESSFUL LOGONS
name: AC-9 (1)

statement

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

guidance

None.
None

SUCCESSFUL AND UNSUCCESSFUL LOGONS

organization-defined time-period
organization-defined time-period
name: AC-9 (2)

statement

Notify the user, upon successful logon/access, of the number of [Selection: successful logons/ accesses; unsuccessful logon/access attempts; both] during .

guidance

None.
None

NOTIFICATION OF ACCOUNT CHANGES

organization-defined security-related characteristics/parameters of the user#s account
organization-defined security-related characteristics/parameters of the user#s account

organization-defined time-period
organization-defined time-period
name: AC-9 (3)

statement

Notify the user, upon successful logon/access, of changes to during .

guidance

None.
None

ADDITIONAL LOGON INFORMATION

organization-defined information to be included in addition to the date and time of the last logon/ access
organization-defined information to be included in addition to the date and time of the last logon/ access
name: AC-9 (4)

statement

Notify the user, upon successful logon/access, of the following additional information: .

guidance

This control enhancement permits organizations to specify additional information to be provided to users upon logon including, for example, the location of last logon. User location is defined as that information which can be determined by systems, for example, Internet Protocol (IP) addresses from which network logons occurred, notifications of local logons, or device identifiers.
None

CONCURRENT SESSION CONTROL

organization-defined account and/or account type
organization-defined account and/or account type

organization-defined number
organization-defined number
name: AC-10

statement

Limit the number of concurrent sessions for each to .

guidance

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

DEVICE LOCK

organization-defined time-period
organization-defined time-period
name: AC-11

statement

item
name: AC-11a.

Prevent further access to the system by initiating a device lock after of inactivity or upon receiving a request from a user; and

item
name: AC-11b.

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

guidance

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 are implemented where session activities can be determined. This is typically at the operating system level, but can also be at the application level. Device locks are not an acceptable substitute for logging out of systems, for example, if organizations require users to log out at the end of workdays.

PATTERN-HIDING DISPLAYS

name: AC-11 (1)

statement

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

guidance

The pattern-hiding display can include static or dynamic images, for example, patterns used with screen savers, photographic images, solid colors, clock, battery life indicator, or a blank screen, with the caveat that controlled unclassified information is not displayed.
None

REQUIRE USER-INITIATED LOCK

name: AC-11 (2)

statement

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

guidance

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

SESSION TERMINATION

organization-defined conditions or trigger events requiring session disconnect
organization-defined conditions or trigger events requiring session disconnect
name: AC-12

statement

Automatically terminate a user session after .

guidance

This control addresses the termination of user-initiated logical sessions in contrast to SC-10 which addresses the termination of network connections that are associated with communications

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

USER-INITIATED LOGOUTS

organization-defined information resources
organization-defined information resources
name: AC-12 (1)

statement

Provide a logout capability for user-initiated communications sessions whenever authentication is used to gain access to .

guidance

Information resources to which users gain access via authentication include, for example, local workstations, databases, and password-protected websites/web-based services.
None

TERMINATION MESSAGE

name: AC-12 (2)

statement

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

guidance

Logout messages for web page access, for example, can be displayed after authenticated sessions have been terminated. However, for some types of interactive sessions including, for example, file transfer protocol (FTP) sessions, systems typically send logout messages as final messages prior to terminating sessions.
None

TIMEOUT WARNING MESSAGE

name: AC-12 (3)

statement

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

guidance

To increase usability, notify users of pending session termination and prompt for activity if users desire to continue the session.
None

SUPERVISION AND REVIEW # ACCESS CONTROL

name: AC-13

statement

Incorporated into AC-2 and AU-6.

PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

organization-defined user actions
organization-defined user actions
name: AC-14

statement

item
name: AC-14a.

Identify that can be performed on the system without identification or authentication consistent with organizational missions and business functions; and

item
name: AC-14b.

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

guidance

This control addresses situations in which organizations determine that no identification or authentication is required in organizational systems. Organizations may allow a limited number of user actions without identification or authentication including, for example, when individuals access public websites or other publicly accessible federal systems, when individuals use mobile phones to receive calls, or when facsimiles are received. Organizations also identify actions that normally require identification or authentication but may under certain circumstances, allow identification or authentication mechanisms to be bypassed. Such bypasses may occur, for example, via a software-readable physical switch that commands bypass of the logon

functionality and is protected from accidental or unmonitored use. This control does not apply to situations where identification and authentication have already occurred and are not repeated, but rather to situations where identification and authentication have not yet occurred. Organizations may decide that there are no user actions that can be performed on organizational systems without identification and authentication and therefore, the values for assignment statements can be none.

NECESSARY USES

name: AC-14 (1)

statement

Incorporated into AC-14.

AUTOMATED MARKING

name: AC-15

statement

Incorporated into MP-3.

SECURITY AND PRIVACY ATTRIBUTES

organization-defined types of security and privacy attributes
organization-defined types of security and privacy attributes

organization-defined security and privacy attribute values
organization-defined security and privacy attribute values

organization-defined security attributes
organization-defined security attributes

organization-defined systems
organization-defined systems

organization-defined values or ranges
organization-defined values or ranges

name: AC-16

statement

item

name: AC-16a.

Provide the means to associate having with information in storage, in process, and/or in transmission;

item
name: AC-16b.

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

item
name: AC-16c.

Establish the permitted for ; and

item
name: AC-16d.

Determine the permitted for each of the established security and privacy attributes.

guidance

Information is represented internally within systems using abstractions known as data structures. Internal data structures can represent different types of entities, both active and passive. Active entities, also known as subjects, are typically associated with individuals, devices, or processes acting on behalf of individuals. Passive entities, also known as objects, are typically associated with data structures such as records, buffers, tables, files, inter-process pipes, and communications ports. Security attributes, a form of metadata, are abstractions representing the basic properties or characteristics of active and passive entities with respect to safeguarding information. Privacy attributes, which may be used independently, or in conjunction with security attributes, represent the basic properties or characteristics of an entity with respect to the management of personally identifiable information. Such attributes are used to enable the implementation of the need for the record in the performance of duties, the identification of personal information within data objects, and the identification of permitted uses of personal information. Attributes can be explicitly or implicitly associated with the information contained in organizational systems or system components. Security and privacy attributes may be associated with active entities (i.e., subjects) that have the potential to send or receive information, to cause information to flow among objects, or to change the system state. These attributes may also be associated with passive entities (i.e., objects) that contain or receive information. The association of security and privacy attributes to subjects and objects is referred to as binding and is inclusive of setting the attribute value and the attribute type. Security and privacy attributes when bound to data or information, enable the enforcement of security policies for access control and information flow control and privacy policies including, for example, for data retention limits and permitted uses of personally identifiable information. Such enforcement occurs through organizational processes or system functions or mechanisms. Binding techniques implemented by systems affect the strength of attribute binding to information. Binding strength and the assurance associated with binding techniques play an important part in the trust

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

DYNAMIC ATTRIBUTE ASSOCIATION

organization-defined subjects and objects
organization-defined subjects and objects

organization-defined security and privacy policies
organization-defined security and privacy policies

name: AC-16 (1)

statement

Dynamically associate security and privacy attributes with in accordance with as information is created and combined.

guidance

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

None

ATTRIBUTE VALUE CHANGES BY AUTHORIZED INDIVIDUALS

name: AC-16 (2)

statement

Provide authorized individuals (or processes acting on behalf of individuals) the capability to define or change the value of associated security and privacy attributes.

guidance

The content or assigned values of security and privacy attributes can directly affect the ability of individuals to access organizational information. Therefore, it is important for systems to be able to limit the ability to create or modify attributes to authorized individuals.
None

MAINTENANCE OF ATTRIBUTE ASSOCIATIONS BY SYSTEM

organization-defined security and privacy attributes
organization-defined security and privacy attributes

organization-defined subjects and objects
organization-defined subjects and objects

name: AC-16 (3)

statement

Maintain the association and integrity of to .

guidance

Maintaining the association and integrity of security and privacy attributes to subjects and objects with sufficient assurance helps to ensure that the attribute associations can be used as the basis of automated policy actions. Automated policy actions include, for example, retention date expirations, access control decisions, and information flow control decisions.
None

ASSOCIATION OF ATTRIBUTES BY AUTHORIZED INDIVIDUALS

organization-defined security and privacy attributes
organization-defined security and privacy attributes

organization-defined subjects and objects
organization-defined subjects and objects

name: AC-16 (4)

statement

Provide the capability to associate with by authorized individuals (or processes acting on behalf of individuals).

guidance

The support provided by systems can include, for example, prompting users to select specific security or privacy attributes to be associated with specific information objects; employing automated mechanisms to categorize information with appropriate security or privacy attributes based on defined policies; or ensuring that the combination of selected security or privacy attributes selected is valid. Organizations consider the creation, deletion, or modification of security and privacy attributes when defining auditable events.
None

ATTRIBUTE DISPLAYS FOR OUTPUT DEVICES

organization-identified special dissemination, handling, or distribution instructions
organization-identified special dissemination, handling, or distribution instructions

organization-identified human-readable, standard naming conventions
organization-identified human-readable, standard naming conventions

name: AC-16 (5)

statement

Display security and privacy attributes in human-readable form on each object that the system transmits to output devices to identify using .

guidance

System outputs include, for example, pages, screens, or equivalent. System output devices include, for example, printers, notebook computers, video displays on workstations, and personal digital assistants. To mitigate the risk of unauthorized exposure of selected information, for example, shoulder surfing, the outputs display full attribute values when unmasked by the subscriber.
None

MAINTENANCE OF ATTRIBUTE ASSOCIATION BY ORGANIZATION

organization-defined security and privacy attributes
organization-defined security and privacy attributes

organization-defined subjects and objects

organization-defined subjects and objects

organization-defined security and privacy policies
organization-defined security and privacy policies
name: AC-16 (6)

statement

Require personnel to associate, and maintain the association of with in accordance with .

guidance

This control enhancement requires individual users (as opposed to the system) to maintain associations of security and privacy attributes with subjects and objects.
None

CONSISTENT ATTRIBUTE INTERPRETATION

name: AC-16 (7)

statement

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

guidance

To enforce security and privacy policies across multiple components in distributed systems, organizations provide a consistent interpretation of the attributes used in access enforcement and flow enforcement decisions. Organizations establish agreements and processes to ensure that all distributed system components implement security and privacy attributes with consistent interpretations in automated access and flow enforcement actions.
None

ASSOCIATION TECHNIQUES AND TECHNOLOGIES

organization-defined techniques and technologies
organization-defined techniques and technologies

organization-defined level of assurance
organization-defined level of assurance
name: AC-16 (8)

statement

Implement with in associating security and privacy attributes to information.

guidance

The association (i.e., binding) of security and privacy attributes to information within systems is important for conducting automated access enforcement and flow enforcement actions. The association of such attributes can be accomplished with technologies and techniques providing different levels of assurance. For example, systems can cryptographically bind attributes to information using digital signatures with the supporting cryptographic keys protected by hardware devices (sometimes known as hardware roots of trust).
None

ATTRIBUTE REASSIGNMENT

organization-defined techniques or procedures
organization-defined techniques or procedures
name: AC-16 (9)

statement

Reassign security and privacy attributes associated with information only via re-grading mechanisms validated using .

guidance

Validated re-grading mechanisms are employed by organizations to provide the requisite levels of assurance for security and privacy attribute reassignment activities. The validation is facilitated by ensuring that re-grading mechanisms are single purpose and of limited function. Since attribute reassignments can directly affect security and privacy policy enforcement actions, using trustworthy re-grading mechanisms is necessary to ensure that such mechanisms perform in a consistent and correct mode of operation.
None

ATTRIBUTE CONFIGURATION BY AUTHORIZED INDIVIDUALS

name: AC-16 (10)

statement

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.

guidance

The content or assigned values of security and privacy attributes can directly affect the ability of individuals to access organizational information. Therefore, it is important for systems to be able to limit the ability to create or modify attributes to authorized individuals only.
None

AUDIT CHANGES

name: AC-16 (11)

statement

Audit changes to security and privacy attributes.

guidance

None.
None

References
FIPS Publication 140-2

REMOTE ACCESS
name: AC-17

statement

item
name: AC-17a.

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

item
name: AC-17b.

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

guidance

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

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

AUTOMATED MONITORING AND CONTROL

name: AC-17 (1)

statement

Monitor and control remote access methods.

guidance

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

PROTECTION OF CONFIDENTIALITY AND INTEGRITY USING ENCRYPTION

name: AC-17 (2)

statement

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

guidance

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

MANAGED ACCESS CONTROL POINTS

organization-defined number
organization-defined number

name: AC-17 (3)

statement

Route all remote accesses through managed network access control points.

guidance

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

PRIVILEGED COMMANDS AND ACCESS

organization-defined needs

organization-defined needs
name: AC-17 (4)

statement

item
name: AC-17 (4)(a)

Authorize the execution of privileged commands and access to security-relevant information via remote access only for ; and

item
name: AC-17 (4)(b)

Document the rationale for such access in the security plan for the system.

guidance

None.

MONITORING FOR UNAUTHORIZED CONNECTIONS

name: AC-17 (5)

statement

Incorporated into SI-4.

PROTECTION OF INFORMATION

name: AC-17 (6)

statement

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

guidance

None.

ADDITIONAL PROTECTION FOR SECURITY FUNCTION ACCESS

name: AC-17 (7)
AC-3(10)

statement

Incorporated into AC-3(10).

DISABLE NONSECURE NETWORK PROTOCOLS

name: AC-17 (8)

statement

Incorporated into CM-7.

DISCONNECT OR DISABLE ACCESS

organization-defined time-period
organization-defined time-period
name: AC-17 (9)

statement

Provide the capability to expeditiously disconnect or disable remote access to the system within .

guidance

This control enhancement requires organizations to have the capability to rapidly disconnect current users remotely accessing the system or disable further remote access. The speed of disconnect or disablement varies based on the criticality of missions or business functions and the need to eliminate immediate or future remote access to systems.
None

References

NIST Special Publication 800-46
NIST Special Publication 800-77
NIST Special Publication 800-113
NIST Special Publication 800-114
NIST Special Publication 800-121

WIRELESS ACCESS

name: AC-18

statement

item

name: AC-18a.

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

item

name: AC-18b.

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

guidance

Wireless technologies include, for example, microwave, packet radio (ultra-high frequency/very high frequency), 802.11x, and Bluetooth. Wireless networks use authentication protocols which provide credential protection and mutual authentication.

AUTHENTICATION AND ENCRYPTION

name: AC-18 (1)

statement

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

guidance

None.

MONITORING UNAUTHORIZED CONNECTIONS

name: AC-18 (2)

statement

Incorporated into SI-4.

DISABLE WIRELESS NETWORKING

name: AC-18 (3)

statement

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

guidance

None.
None

RESTRICT CONFIGURATIONS BY USERS

name: AC-18 (4)

statement

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

guidance

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

ANTENNAS AND TRANSMISSION POWER LEVELS

name: AC-18 (5)

statement

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.

guidance

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

References

NIST Special Publication 800-48
NIST Special Publication 800-94
NIST Special Publication 800-97

ACCESS CONTROL FOR MOBILE DEVICES

name: AC-19

statement

item
name: AC-19a.

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

item
name: AC-19b.

Authorize the connection of mobile devices to organizational systems; and

item
name: AC-19c.

Protect and control mobile devices when outside of controlled areas.

guidance

A mobile device is a computing device that has a small form factor such that it can easily be carried by a single individual; is designed to operate without a physical connection; possesses local, non-removable or removable data storage; and includes a self-contained power source. Mobile device functionality may also include voice communication capabilities, on-board sensors that allow the device to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, E-readers, and tablets. Mobile devices are typically associated with a single individual and the device is usually near the individual; however, the degree of proximity can vary depending upon on the form factor and size of the device. The processing, storage, and transmission capability of the mobile device may be comparable to or merely a subset of notebook/desktop systems, depending upon the nature and intended purpose of the device. Controlled areas are areas or spaces for which organizations provide sufficient physical or procedural safeguards to meet the requirements established for protecting information and systems. Due to the large variety of mobile devices with different characteristics and capabilities, organizational restrictions may vary for the different classes/types of such devices. Usage restrictions and specific implementation guidance for mobile devices include, for example, configuration management, device identification and authentication, implementation of mandatory protective software, 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 the organizational network and impose a set of usage restrictions while a system owner may withhold authorization for mobile device connection to specific applications or may impose additional usage restrictions before allowing mobile device connections to a system. The need to provide adequate security for mobile devices goes beyond the requirements in this control. Many safeguards for mobile devices are reflected in other security controls allocated to the initial control baselines as starting points for the development of security plans and overlays using the tailoring process. There may also be some overlap by the security controls within the different families of controls. AC-20 addresses mobile devices that are not organization-controlled.

USE OF WRITABLE AND PORTABLE STORAGE DEVICES

name: AC-19 (1)

statement

Incorporated into MP-7.

USE OF PERSONALLY OWNED PORTABLE STORAGE DEVICES

name: AC-19 (2)

statement

Incorporated into MP-7.

USE OF PORTABLE STORAGE DEVICES WITH NO IDENTIFIABLE OWNER

name: AC-19 (3)

statement

Incorporated into MP-7.

RESTRICTIONS FOR CLASSIFIED INFORMATION

organization-defined security officials
organization-defined security officials

organization-defined security policies
organization-defined security policies

name: AC-19 (4)

statement

item
name: AC-19 (4)(a)

Prohibit the use of unclassified mobile devices in facilities containing systems processing, storing, or transmitting classified information unless specifically permitted by the authorizing official; and

item
name: AC-19 (4)(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:

item
name: AC-19 (4)(b)(1)

Connection of unclassified mobile devices to classified systems is prohibited;

item
name: AC-19 (4)(b)(2)

Connection of unclassified mobile devices to unclassified systems requires approval from the authorizing official;

item
name: AC-19 (4)(b)(3)

Use of internal or external modems or wireless interfaces within the unclassified mobile devices is prohibited; and

item
name: AC-19 (4)(b)(4)

Unclassified mobile devices and the information stored on those devices are subject to random reviews and inspections by , and if classified information is found, the incident handling policy is followed.

item
name: AC-19 (4)(c)

Restrict the connection of classified mobile devices to classified systems in accordance with .

guidance

None.

FULL DEVICE AND CONTAINER-BASED ENCRYPTION

organization-defined mobile devices
organization-defined mobile devices
name: AC-19 (5)

statement

Employ [Selection: full-device encryption; container encryption] to protect the confidentiality and integrity of information on .

guidance

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

References

NIST Special Publication 800-114
NIST Special Publication 800-124
NIST Special Publication 800-164

USE OF EXTERNAL SYSTEMS

name: AC-20

statement

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

item
name: AC-20a.

Access the system from external systems; and

item
name: AC-20b.

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

guidance

External systems are systems or components of systems that are outside of the authorization boundary established by organizations and for which organizations typically have no direct supervision and authority over the application of required security controls or the assessment of control effectiveness. External systems include, for example, personally owned systems, components, or devices; privately owned computing and communications devices in commercial or public facilities; systems owned or controlled by nonfederal organizations; and federal systems that are not owned by, operated by, or under the direct supervision and authority of the organization. This includes systems managed by contractors, systems owned by other federal agencies, and systems owned by other organizations within the same agency. This control addresses the use of external systems for the processing, storage, or transmission of organizational information, including, for example, accessing cloud services from organizational systems. For some external systems (i.e., systems operated by other federal agencies and organizations subordinate to those agencies), the trust relationships that have been established between those organizations and the originating organization may be such, that no explicit terms and conditions are required. Systems within these organizations may not be considered external. These situations occur when, for example, there are pre-existing sharing and trust agreements (either implicit or explicit) established between federal agencies or organizations subordinate to those agencies, or when such trust agreements are specified by applicable laws, Executive Orders, directives, regulations, or policies. Authorized individuals include, for example, organizational personnel, contractors, or other individuals with authorized access to organizational systems and over which organizations have the authority to impose specific rules of behavior with regard to system access. Restrictions that organizations impose on authorized individuals need not be uniform, as those restrictions may vary depending on the trust relationships between organizations. Therefore, organizations may choose to impose different security restrictions on contractors than on state, local, or tribal governments. This control does not apply to external systems used to access public interfaces to organizational systems. Organizations establish specific terms and conditions for the use of external systems in accordance with organizational security policies and procedures. Terms and conditions address as a minimum: the specific types of applications that can be accessed on organizational systems

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

LIMITS ON AUTHORIZED USE

name: AC-20 (1)

statement

Permit authorized individuals to use an external system to access the system or to process, store, or transmit organization-controlled information only after:

item

name: AC-20 (1)(a)

Verification of the implementation of required security and privacy controls on the external system as specified in the organization#s security and privacy policies and security and privacy plans; or

item

name: AC-20 (1)(b)

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

guidance

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

PORTABLE STORAGE DEVICES

organization-defined restrictions
organization-defined restrictions

name: AC-20 (2)

statement

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

guidance

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

NON-ORGANIZATIONALLY OWNED SYSTEMS AND COMPONENTS

organization-defined restrictions
organization-defined restrictions
name: AC-20 (3)

statement

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

guidance

Non-organizationally owned systems or system components include systems or system components owned by other organizations and personally owned devices. There are potential risks to using non-organizationally owned systems or system components. In some cases, the risk is sufficiently high as to prohibit such use. In other cases, the use of such systems or system components may be allowed but restricted in some way. Restrictions include, for example, requiring the implementation of approved security and privacy controls prior to authorizing the connection of non-organizationally owned systems and components; limiting access to certain types of information, services, or applications; using virtualization techniques to limit processing and storage activities to servers or other system components provisioned by the organization; and agreeing to the specified terms and conditions for usage. Organizations consult with the Office of the General Counsel regarding any legal issues associated with using personally owned devices, including, for example, requirements for conducting forensic analyses during investigations after an incident.
None

NETWORK ACCESSIBLE STORAGE DEVICES

organization-defined network accessible storage devices
organization-defined network accessible storage devices
name: AC-20 (4)

statement

Prohibit the use of in external systems.

guidance

Network accessible storage devices in external systems include, for example, online storage devices in public, hybrid, or community cloud-based systems.
None

References
FIPS Publication 199

INFORMATION SHARING

organization-defined information sharing circumstances where user discretion is required
organization-defined information sharing circumstances where user discretion is required

organization-defined automated mechanisms or manual processes
organization-defined automated mechanisms or manual processes
name: AC-21

statement

item
name: AC-21a.

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

item
name: AC-21b.

Employ to assist users in making information sharing and collaboration decisions.

guidance

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

AUTOMATED DECISION SUPPORT

name: AC-21 (1)

statement

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

guidance

None.
None

INFORMATION SEARCH AND RETRIEVAL

organization-defined information sharing restrictions
organization-defined information sharing restrictions
name: AC-21 (2)

statement

Implement information search and retrieval services that enforce .

guidance

None.
None

PUBLICLY ACCESSIBLE CONTENT

organization-defined frequency
organization-defined frequency
name: AC-22

statement

item
name: AC-22a.

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

item
name: AC-22b.

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

item
name: AC-22c.

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

item
name: AC-22d.

Review the content on the publicly accessible system for nonpublic information and remove such information, if discovered.

guidance

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

DATA MINING PROTECTION

organization-defined data mining prevention and detection techniques
organization-defined data mining prevention and detection techniques

organization-defined data storage objects
organization-defined data storage objects
name: AC-23

statement

Employ for to detect and protect against unauthorized data mining.

guidance

Data storage objects include, for example, databases, database records, and database fields. Data mining prevention and detection techniques include, for example, limiting the types of responses provided to database queries; limiting the number and the frequency of database queries to increase the work factor needed to determine the contents of such databases; and notifying organizational personnel when atypical database queries or accesses occur. This control focuses on the protection of organizational information from data mining while such information resides in organizational data stores. In contrast, AU-13 focuses on monitoring for organizational information that may have been mined or otherwise obtained from data stores and is now available as open source information residing on external sites, for example, through social networking or social media websites.
None

ACCESS CONTROL DECISIONS

organization-defined access control decisions
organization-defined access control decisions
name: AC-24

statement

Establish procedures to ensure are applied to each access request prior to access enforcement.

guidance

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

TRANSMIT ACCESS AUTHORIZATION INFORMATION

organization-defined access authorization information
organization-defined access authorization information

organization-defined security safeguards
organization-defined security safeguards

organization-defined systems
organization-defined systems
name: AC-24 (1)

statement

Transmit using to that enforce access control decisions.

guidance

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

None

NO USER OR PROCESS IDENTITY

organization-defined security attributes
organization-defined security attributes
name: AC-24 (2)

statement

Enforce access control decisions based on that do not include the identity of the user or process acting on behalf of the user.

guidance

In certain situations, it is important that access control decisions can be made without information regarding the identity of the users issuing the requests. These are generally instances where preserving individual privacy is of paramount importance. In other situations, user identification information is simply not needed for access control decisions and, especially in the case of distributed systems, transmitting such information with the needed degree of assurance may be very expensive or difficult to accomplish.
None

REFERENCE MONITOR

organization-defined access control policies
organization-defined access control policies
name: AC-25

statement

Implement a reference monitor for that is tamperproof, always invoked, and small enough to be subject to analysis and testing, the completeness of which can be assured.

guidance

Information is represented internally within systems using abstractions known as data structures. Internal data structures can represent different types of entities, both active and passive. Active entities, also known as subjects, are associated with individuals, devices, or processes acting on behalf of individuals. Passive entities, also known as objects, are typically associated with data structures such as records, buffers, tables, files, inter-process pipes, and communications ports. Reference monitors enforce mandatory access control policies, a type of access control that restricts access to objects based on the identity of subjects or groups to which the subjects belong. The access controls are mandatory because subjects with certain privileges (i.e., access permissions) are restricted from passing those privileges on to any other subjects, either directly or indirectly#that is, the system strictly enforces the access control policy based on the rule

set established by the policy. The tamperproof property of the reference monitor prevents adversaries from compromising the functioning of the mechanism. The always invoked property prevents adversaries from bypassing the mechanism and hence violating the security policy. The smallness property helps to ensure the completeness in the analysis and testing of the mechanism to detect weaknesses or deficiencies (i.e., latent flaws) that would prevent the enforcement of the security policy.

AWARENESS AND TRAINING

AWARENESS AND TRAINING POLICY AND PROCEDURES

organization-defined personnel or roles
organization-defined personnel or roles

organization-defined senior management official
organization-defined senior management official

organization-defined frequency
organization-defined frequency

organization-defined frequency
organization-defined frequency
name: AT-1

statement

item
name: AT-1a.

Develop, document, and disseminate to :

item
name: AT-1a.1.

A security and privacy awareness and training policy that:

item
name: AT-1a.1.(a)

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

item
name: AT-1a.1.(b)

Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and

item
name: AT-1a.2.

Procedures to facilitate the implementation of the security and privacy awareness and training policy and the associated security and privacy awareness and training controls;

item
name: AT-1b.

Designate an to manage the security and privacy awareness and training policy and procedures;

item
name: AT-1c.

Review and update the current security and privacy awareness and training:

item
name: AT-1c.1.

Policy ; and

item
name: AT-1c.2.

Procedures ;

item
name: AT-1d.

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

item
name: AT-1e.

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

guidance

This control addresses the establishment of policy and procedures for the effective implementation of the controls and control enhancements in the AT family. The risk management strategy is an important factor in establishing policy and procedures. Comprehensive policy and procedures help provide security and privacy assurance. Security and privacy program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general

security and privacy policy or can be represented by multiple policies reflecting the complex nature of organizations. The procedures can be established for security and privacy programs and for systems, if needed. Procedures describe how policies or controls are implemented and can be directed at the personnel or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. It is important to recognize that restating controls does not constitute an organizational policy or procedure.

References

NIST Special Publication 800-12
NIST Special Publication 800-30
NIST Special Publication 800-39
NIST Special Publication 800-50
NIST Special Publication 800-100

AWARENESS TRAINING

organization-defined frequency
organization-defined frequency
name: AT-2

statement

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

item
name: AT-2a.

As part of initial training for new users;

item
name: AT-2b.

When required by system changes; and

item
name: AT-2c.

thereafter.

guidance

Organizations determine the content of security and privacy awareness training and security and privacy awareness techniques based on the specific organizational requirements and the systems to which personnel have authorized access. The content includes an understanding

of the need for information security and privacy and actions by users to maintain security and privacy and to respond to suspected security and privacy incidents. The content also addresses an awareness of the need for operations security. Security and privacy awareness techniques can include, for example, displaying posters, offering supplies inscribed with security and privacy reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting information security and privacy awareness events. Awareness training after the initial training (i.e., described AT-2c) is conducted at a minimum frequency consistent with applicable laws, directives, regulations, and policies. Such training may be satisfied by one or more short ad hoc sessions and include topical information on recent attack schemes, changes to organizational security and privacy policies, revised security and privacy expectations, and/or a subset of topics from the initial training.

PRACTICAL EXERCISES

name: AT-2 (1)

statement

Include practical exercises in awareness training that simulate security and privacy incidents.

guidance

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

INSIDER THREAT

name: AT-2 (2)

statement

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

guidance

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

SOCIAL ENGINEERING AND MINING

name: AT-2 (3)

statement

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

guidance

Social engineering is an attempt to trick someone into revealing information or taking an action that can be used to attack or compromise systems. Examples of social engineering include phishing, pretexting, baiting, quid pro quo, and tailgaiting. Social mining is an attempt, in a social setting, to gather information about the organization that may support future attacks. Security and privacy awareness training includes information on how to communicate concerns of employees and management regarding potential and actual instances of social engineering and mining through organizational channels based on established policies and procedures.
None

References

NIST Special Publication 800-50

ROLE-BASED TRAINING

organization-defined roles and responsibilities
organization-defined roles and responsibilities

organization-defined frequency
organization-defined frequency
name: AT-3

statement

Provide role-based security and privacy training to personnel with the following roles and responsibilities: :

item
name: AT-3a.

Before authorizing access to the system or performing assigned duties;

item
name: AT-3b.

When required by system changes; and

item
name: AT-3c.

thereafter.

guidance

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

ENVIRONMENTAL CONTROLS

organization-defined personnel or roles
organization-defined personnel or roles

organization-defined frequency
organization-defined frequency
name: AT-3 (1)

statement

Provide with initial and training in the employment and operation of environmental controls.

guidance

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

PHYSICAL SECURITY CONTROLS

organization-defined personnel or roles

organization-defined personnel or roles

organization-defined frequency
organization-defined frequency
name: AT-3 (2)

statement

Provide with initial and training in the employment and operation of physical security controls.

guidance

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

PRACTICAL EXERCISES

name: AT-3 (3)

statement

Include practical exercises in security and privacy training that reinforce training objectives.

guidance

Practical exercises for security may include, for example, security training for software developers that includes simulated cyber-attacks exploiting common software vulnerabilities, or spear/whale phishing attacks targeted at senior leaders/executives. Practical exercises for privacy may include, for example, practice modules with quizzes on handling personally identifiable information in various scenarios, and model scenarios on conducting privacy impact assessments.

None

SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR

organization-defined indicators of malicious code
organization-defined indicators of malicious code
name: AT-3 (4)

statement

Provide training to personnel on to recognize suspicious communications and anomalous behavior in organizational systems.

guidance

A well-trained workforce provides another organizational safeguard that can be employed as part of a defense-in-depth strategy to protect organizations against malicious code coming in to organizations via email or the web applications. Personnel are trained to look for indications of potentially suspicious email for example, receiving an unexpected email, receiving an email containing strange or poor grammar, or receiving an email from an unfamiliar sender but who appears to be from a known sponsor or contractor. Personnel are also trained on how to respond to suspicious email or web communications. For this process to work effectively, organizational personnel are trained and made aware of what constitutes suspicious communications. Training personnel on how to recognize anomalous behaviors in organizational systems can potentially provide early warning for the presence of malicious code. Recognition of such anomalous behavior by organizational personnel can supplement automated malicious code detection and protection tools and systems employed by organizations.
None

PERSONALLY IDENTIFIABLE INFORMATION PROCESSING

organization-defined frequency
organization-defined frequency
name: AT-3 (5)

statement

Provide personnel who process personally identifiable information with initial and training on:

item
name: AT-3 (5)(a)

Organizational authority for collecting personally identifiable information;

item
name: AT-3 (5)(b)

Authorized uses of personally identifiable information;

item
name: AT-3 (5)(c)

Content of System of Records Notices;

item
name: AT-3 (5)(d)

Authorized sharing of personally identifiable information with external parties; and

item
name: AT-3 (5)(e)

Consequences of unauthorized use or sharing of personally identifiable information.

guidance

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

References
NIST Special Publication 800-50

TRAINING RECORDS

organization-defined time-period
organization-defined time-period
name: AT-4

statement

item
name: AT-4a.

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

item
name: AT-4b.

Retain individual training records for .

guidance

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

CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS
name: AT-5

statement

Incorporated into PM-15.

AUDIT AND ACCOUNTABILITY

AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES

organization-defined personnel or roles
organization-defined personnel or roles

organization-defined senior management official
organization-defined senior management official

organization-defined frequency
organization-defined frequency

organization-defined frequency
organization-defined frequency
name: AU-1

statement

item
name: AU-1a.

Develop, document, and disseminate to :

item
name: AU-1a.1.

An audit and accountability policy that:

item
name: AU-1a.1.(a)

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

item
name: AU-1a.1.(b)

Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and

item
name: AU-1a.2.

Procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls;

item
name: AU-1b.

Designate an to manage the audit and accountability policy and procedures;

item
name: AU-1c.

Review and update the current audit and accountability:

item
name: AU-1c.1.

Policy ; and

item
name: AU-1c.2.

Procedures ;

item
name: AU-1d.

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

item
name: AU-1e.

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

guidance

This control addresses the establishment of policy and procedures for the effective implementation of the controls and control enhancements in the AU family. The risk management strategy is an important factor in establishing policy and procedures. Comprehensive policy and procedures help provide security and privacy assurance. Security and privacy program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general security and privacy policy or can be represented by multiple policies reflecting the complex nature of organizations. The procedures can be established for security and privacy programs and for systems, if needed. Procedures describe how policies or controls are implemented and can be directed at the personnel or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. It is important to recognize that restating controls does not constitute an organizational policy or procedure.

References
NIST Special Publication 800-12
NIST Special Publication 800-30
NIST Special Publication 800-39
NIST Special Publication 800-50
NIST Special Publication 800-100

AUDIT EVENTS

organization-defined auditable event types
organization-defined auditable event types

organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event
organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event
name: AU-2

statement

item
name: AU-2a.

Verify that the system can audit the following event types: ;

item
name: AU-2b.

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

item
name: AU-2c.

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

item
name: AU-2d.

Specify that the following event types are to be audited within the system: .

guidance

An event is any observable occurrence in an organizational system. Organizations identify audit event types as those events which are significant and relevant to the security of systems and

the environments in which those systems operate to meet specific and ongoing audit needs. Audit event types can include, for example, password changes; failed logons or failed accesses related to systems; security attribute changes, administrative privilege usage, PIV credential usage, query parameters, or external credential usage. In determining the set of auditable event types, organizations consider the auditing appropriate for each of the security controls to be implemented. To balance auditing requirements with other system needs, this control also requires identifying that subset of auditable event types that are audited at a given point in time. For example, organizations may determine that systems must have the capability to log every file access both successful and unsuccessful, but not activate that capability except for specific circumstances due to the potential burden on system performance. Auditing requirements, including the need for auditable events, may be referenced in other security and privacy controls and control enhancements for example, AC-2(4), AC-3(10), AC-6(9), AC-16(11), AC-17(1), CM-3.f, CM-5(1), IA-3(3.b), MA-4(1), MP-4(2), PA-4.d, PE-3, PM-22, RA-8, SC-7(9), SC-7(15), SI-3(8), SI-4(22), SI-7(8), and SI-10(1). Organizations also include auditable event types that are required by applicable laws, Executive Orders, directives, policies, regulations, standards, and guidelines. Audit records can be generated at various levels, including at the packet level as information traverses the network. Selecting the appropriate level of auditing is an important aspect of an audit capability and can facilitate the identification of root causes to problems. Organizations consider in the definition of auditable event types, the auditing necessary to cover related event types such as the steps in distributed, transaction-based processes and actions that occur in service-oriented architectures.

COMPILATION OF AUDIT RECORDS FROM MULTIPLE SOURCES

name: AU-2 (1)

statement

Incorporated into AU-12.

SELECTION OF AUDIT EVENTS BY COMPONENT

name: AU-2 (2)

statement

Incorporated into AU-12.

REVIEWS AND UPDATES

organization-defined frequency
organization-defined frequency

name: AU-2 (3)

statement

Review and update the audited events .

guidance

Over time, the events that organizations believe should be audited may change. Reviewing and updating the set of audited events periodically is necessary to ensure that the current set is still necessary and sufficient.
None

PRIVILEGED FUNCTIONS

name: AU-2 (4)
AC-6(9)

statement

Incorporated into AC-6(9).

References
NIST Special Publication 800-92

CONTENT OF AUDIT RECORDS

name: AU-3

statement

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

guidance

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

ADDITIONAL AUDIT INFORMATION

organization-defined additional, more detailed information
organization-defined additional, more detailed information
name: AU-3 (1)

statement

Generate audit records containing the following additional information: .

guidance

Implementation of this control enhancement is dependent on system functionality to configure audit record content. Detailed information that organizations may consider in audit records includes, for example, full text recording of privileged commands or the individual identities of group account users. Organizations consider limiting the additional audit information to only that information explicitly needed for specific audit requirements. This facilitates the use of audit trails and audit logs by not including information that could potentially be misleading or could make it more difficult to locate information of interest.
None

CENTRALIZED MANAGEMENT OF PLANNED AUDIT RECORD CONTENT

organization-defined system components
organization-defined system components
name: AU-3 (2)

statement

Provide centralized management and configuration of the content to be captured in audit records generated by .

guidance

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

LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS

organization-defined elements
organization-defined elements
name: AU-3 (3)

statement

Limit personally identifiable information contained in audit records to the following elements identified in the privacy risk assessment: .

guidance

Limiting personally identifiable information in audit records when such information is not needed for operational purposes helps reduce the level of privacy risk created by a system.
None

AUDIT STORAGE CAPACITY

organization-defined audit record retention requirements
organization-defined audit record retention requirements
name: AU-4

statement

Allocate audit record storage capacity to accommodate .

guidance

Organizations consider the types of auditing to be performed and the audit processing requirements when allocating audit storage capacity. Allocating sufficient audit storage capacity reduces the likelihood of such capacity being exceeded and resulting in the potential loss or reduction of auditing capability.

TRANSFER TO ALTERNATE STORAGE

organization-defined frequency
organization-defined frequency
name: AU-4 (1)

statement

Off-load audit records onto a different system or media than the system being audited.

guidance

Off-loading is a process designed to preserve the confidentiality and integrity of audit records by moving the records from the primary system to a secondary or alternate system. It is a common process in systems with limited audit storage capacity; the audit storage is used only in a transitory fashion until the system can communicate with the secondary or alternate system designated for storing the audit records, at which point the information is transferred.
None

RESPONSE TO AUDIT PROCESSING FAILURES

organization-defined personnel or roles
organization-defined personnel or roles

organization-defined time-period
organization-defined time-period

organization-defined actions to be taken

organization-defined actions to be taken
name: AU-5

statement

item
name: AU-5a.

Alert in the event of an audit processing failure within ; and

item
name: AU-5b.

Take the following additional actions: .

guidance

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

AUDIT STORAGE CAPACITY

organization-defined personnel, roles, and/or locations
organization-defined personnel, roles, and/or locations

organization-defined time-period
organization-defined time-period

organization-defined percentage
organization-defined percentage
name: AU-5 (1)

statement

Provide a warning to within when allocated audit record storage volume reaches of repository maximum audit record storage capacity.

guidance

Organizations may have multiple audit data storage repositories distributed across multiple system components, with each repository having different storage volume capacities.
None

REAL-TIME ALERTS

organization-defined real-time-period
organization-defined real-time-period

organization-defined personnel, roles, and/or locations
organization-defined personnel, roles, and/or locations

organization-defined audit failure events requiring real-time alerts
organization-defined audit failure events requiring real-time alerts
name: AU-5 (2)

statement

Provide an alert in to when the following audit failure events occur: .

guidance

Alerts provide organizations with urgent messages. Real-time alerts provide these messages at information technology speed (i.e., the time from event detection to alert occurs in seconds or less).
None

CONFIGURABLE TRAFFIC VOLUME THRESHOLDS

name: AU-5 (3)

statement

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

guidance

Organizations have the capability to reject or delay the processing of network communications traffic if auditing such traffic is determined to exceed the storage capacity of the system audit function. The rejection or delay response is triggered by the established organizational traffic volume thresholds which can be adjusted based on changes to audit storage capacity.
None

SHUTDOWN ON FAILURE

organization-defined audit failures
organization-defined audit failures
name: AU-5 (4)

statement

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

guidance

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

AUDIT REVIEW, ANALYSIS, AND REPORTING

organization-defined frequency
organization-defined frequency

organization-defined inappropriate or unusual activity
organization-defined inappropriate or unusual activity

organization-defined personnel or roles
organization-defined personnel or roles
name: AU-6

statement

item
name: AU-6a.

Review and analyze system audit records for indications of ;

item
name: AU-6b.

Report findings to ; and

item
name: AU-6c.

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

guidance

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

AUTOMATED PROCESS INTEGRATION

name: AU-6 (1)

statement

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

guidance

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

AUTOMATED SECURITY ALERTS

name: AU-6 (2)

statement

Incorporated into SI-4.

CORRELATE AUDIT REPOSITORIES

name: AU-6 (3)

statement

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

guidance

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

CENTRAL REVIEW AND ANALYSIS

name: AU-6 (4)

statement

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

guidance

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

INTEGRATED ANALYSIS OF AUDIT RECORDS

organization-defined data/information collected from other sources
organization-defined data/information collected from other sources

name: AU-6 (5)

statement

Integrate analysis of audit records with analysis of [Selection (one or more): vulnerability scanning information; performance data; system monitoring information;] to further enhance the ability to identify inappropriate or unusual activity.

guidance

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

CORRELATION WITH PHYSICAL MONITORING

name: AU-6 (6)

statement

Correlate information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.

guidance

The correlation of physical audit information and audit logs from systems may assist organizations in identifying examples of suspicious behavior or supporting evidence of such behavior. For example, the correlation of an individual#s identity for logical access to certain systems with the additional physical security information that the individual was present at the facility when the logical access occurred, may be useful in investigations.
None

PERMITTED ACTIONS

name: AU-6 (7)

statement

Specify the permitted actions for each [Selection (one or more): system process; role; user] associated with the review, analysis, and reporting of audit information.

guidance

Organizations specify permitted actions for system processes, roles, and/or users associated with the review, analysis, and reporting of audit records through account management techniques. Specifying permitted actions on audit information is a way to enforce the principle of least privilege. Permitted actions are enforced by the system and include, for example, read, write, execute, append, and delete.
None

FULL TEXT ANALYSIS OF PRIVILEGED COMMANDS

name: AU-6 (8)

statement

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

guidance

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

CORRELATION WITH INFORMATION FROM NONTECHNICAL SOURCES

name: AU-6 (9)

statement

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

guidance

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

AUDIT LEVEL ADJUSTMENT

name: AU-6 (10)

statement

Incorporated into AU-6.

AUDIT REDUCTION AND REPORT GENERATION

name: AU-7

statement

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

item

name: AU-7a.

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

item

name: AU-7b.

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

guidance

Audit reduction is a process that manipulates collected audit information and organizes such information in a summary format that is more meaningful to analysts. Audit reduction and report generation capabilities do not always emanate from the same system or from the same organizational entities conducting auditing activities. Audit reduction capability can include, for example, modern data mining techniques with advanced data filters to identify anomalous behavior in audit records. The report generation capability provided by the system can generate customizable reports. Time ordering of audit records can be a significant issue if the granularity of the timestamp in the record is insufficient.

AUTOMATIC PROCESSING

organization-defined audit fields within audit records
organization-defined audit fields within audit records
name: AU-7 (1)

statement

Provide and implement the capability to process audit records for events of interest based on .

guidance

Events of interest can be identified by the content of specific audit record fields including, for example, identities of individuals, event types, event locations, event times, event dates, system resources involved, Internet Protocol addresses involved, or information objects accessed. Organizations may define audit event criteria to any degree of granularity required, for example, locations selectable by general networking location or selectable by specific system component.
None

AUTOMATIC SORT AND SEARCH

organization-defined audit fields within audit records
organization-defined audit fields within audit records
name: AU-7 (2)

statement

Provide and implement the capability to sort and search audit records for events of interest based on the content of .

guidance

Sorting and searching of audit records may be based upon the contents of audit record fields, for example, date and time of events; user identifiers; Internet Protocol addresses involved in the event; type of event; or event success or failure.
None

TIME STAMPS

organization-defined granularity of time measurement
organization-defined granularity of time measurement
name: AU-8

statement

item
name: AU-8a.

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

item
name: AU-8b.

Record time stamps for audit records that can be mapped to Coordinated Universal Time or Greenwich Mean Time and meets .

guidance

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

SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE

organization-defined frequency
organization-defined frequency

organization-defined authoritative time source
organization-defined authoritative time source

organization-defined time-period
organization-defined time-period
name: AU-8 (1)

statement

item
name: AU-8 (1)(a)

Compare the internal system clocks with ; and

item
name: AU-8 (1)(b)

Synchronize the internal system clocks to the authoritative time source when the time difference is greater than .

guidance

This control enhancement provides uniformity of time stamps for systems with multiple system clocks and systems connected over a network.
None

SECONDARY AUTHORITATIVE TIME SOURCE
name: AU-8 (2)

statement

item
name: AU-8 (2)(a)

Identify a secondary authoritative time source that is in a different geographic region than the primary authoritative time source; and

item
name: AU-8 (2)(b)

Synchronize the internal system clocks to the secondary authoritative time source if the primary authoritative time source is unavailable.

guidance

It may be necessary to employ geolocation information to determine that the secondary authoritative time source is in a different geographic region.
None

PROTECTION OF AUDIT INFORMATION
name: AU-9

statement

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

guidance

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

HARDWARE WRITE-ONCE MEDIA

name: AU-9 (1)

statement

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

guidance

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

STORE ON SEPARATE PHYSICAL SYSTEMS OR COMPONENTS

organization-defined frequency
organization-defined frequency
name: AU-9 (2)

statement

Store audit records in a repository that is part of a physically different system or system component than the system or component being audited.

guidance

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

CRYPTOGRAPHIC PROTECTION

name: AU-9 (3)

statement

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

guidance

Cryptographic mechanisms used for protecting the integrity of audit information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the secret key used to generate the hash.

ACCESS BY SUBSET OF PRIVILEGED USERS

organization-defined subset of privileged users
organization-defined subset of privileged users
name: AU-9 (4)

statement

Authorize access to management of audit functionality to only .

guidance

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

DUAL AUTHORIZATION

organization-defined audit information
organization-defined audit information
name: AU-9 (5)

statement

Enforce dual authorization for [Selection (one or more): movement; deletion] of .

guidance

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

READ ONLY ACCESS

organization-defined subset of privileged users
organization-defined subset of privileged users
name: AU-9 (6)

statement

Authorize read-only access to audit information to .

guidance

Restricting privileged user authorizations to read-only helps to limit the potential damage to organizations that could be initiated by such users, for example, deleting audit records to cover up malicious activity.
None

STORE ON COMPONENT WITH DIFFERENT OPERATING SYSTEM

name: AU-9 (7)

statement

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

guidance

This control enhancement helps reduce the risk of a vulnerability specific to an operating system resulting in a compromise of the audit records. Related controls: AU-4, AU-5, AU-11, SC-29.

References

FIPS Publication 140-2

NON-REPUDIATION

organization-defined actions to be covered by non-repudiation
organization-defined actions to be covered by non-repudiation
name: AU-10

statement

Protect against an individual (or process acting on behalf of an individual) falsely denying having performed .

guidance

Types of individual actions covered by non-repudiation include creating information, sending and receiving messages, and approving information. Non-repudiation protects individuals against later claims by authors of not having authored certain documents; senders of not having transmitted messages; receivers of not having received messages; and individual signatories of not having signed documents. Non-repudiation services can be used to determine if information originated from a certain individual, or if an individual took specific actions, for example,

sending an email, signing a contract, or approving a procurement request, or received specific information. Organizations obtain non-repudiation services by employing various techniques or mechanisms including, for example, digital signatures and digital message receipts.

ASSOCIATION OF IDENTITIES

organization-defined strength of binding
organization-defined strength of binding
name: AU-10 (1)

statement

item
name: AU-10 (1)(a)

Bind the identity of the information producer with the information to ; and

item
name: AU-10 (1)(b)

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

guidance

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

VALIDATE BINDING OF INFORMATION PRODUCER IDENTITY

organization-defined frequency
organization-defined frequency

organization-defined actions
organization-defined actions
name: AU-10 (2)

statement

item
name: AU-10 (2)(a)

Validate the binding of the information producer identity to the information at ; and

item
name: AU-10 (2)(b)

Perform in the event of a validation error.

guidance

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

CHAIN OF CUSTODY

name: AU-10 (3)

statement

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

guidance

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

VALIDATE BINDING OF INFORMATION REVIEWER IDENTITY

organization-defined security domains
organization-defined security domains

organization-defined actions
organization-defined actions
name: AU-10 (4)

statement

item
name: AU-10 (4)(a)

Validate the binding of the information reviewer identity to the information at the transfer or release points prior to release or transfer between ; and

item
name: AU-10 (4)(b)

Perform in the event of a validation error.

guidance

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

DIGITAL SIGNATURES

name: AU-10 (5)

statement

Incorporated into SI-13.

References

FIPS Publication 140-2

AUDIT RECORD RETENTION

organization-defined time-period consistent with records retention policy

organization-defined time-period consistent with records retention policy

name: AU-11

statement

Retain audit records for to provide support for after-the-fact investigations of security and privacy incidents and to meet regulatory and organizational information retention requirements.

guidance

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

LONG-TERM RETRIEVAL CAPABILITY

organization-defined measures
organization-defined measures
name: AU-11 (1)

statement

Employ to ensure that long-term audit records generated by the system can be retrieved.

guidance

This control enhancement helps to ensure that, from a technological perspective, audit records requiring long-term storage (on the order of years) can be accessed and read when needed. Measures employed by organizations to help facilitate the retrieval of audit records include, for example, converting records to newer formats, retaining equipment capable of reading the records, and retaining necessary documentation to help organizational personnel understand how to interpret the records.
None

AUDIT GENERATION

organization-defined system components
organization-defined system components

organization-defined personnel or roles
organization-defined personnel or roles
name: AU-12

statement

item
name: AU-12a.

Provide audit record generation capability for the auditable event types in AU-2 a. at ;

item
name: AU-12b.

Allow to select which auditable event types are to be audited by specific components of the system; and

item
name: AU-12c.

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

guidance

Audit records can be generated from many different system components. The list of audited event types is the set of event types for which audits are to be generated. These event types are a subset of all event types for which the system can generate audit records.
PM-12 SC-18

SYSTEM-WIDE AND TIME-CORRELATED AUDIT TRAIL

organization-defined system components
organization-defined system components

organization-defined level of tolerance for the relationship between time stamps of individual records in the audit trail
organization-defined level of tolerance for the relationship between time stamps of individual records in the audit trail
name: AU-12 (1)

statement

Compile audit records from into a system-wide (logical or physical) audit trail that is time-correlated to within .

guidance

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

STANDARDIZED FORMATS

name: AU-12 (2)

statement

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

guidance

Audit information that is normalized to common standards promotes interoperability and exchange of such information between dissimilar devices and systems. This facilitates production of event information that can be more readily analyzed and correlated. Standard formats for audit records include, for example, system log records and audit records compliant with Common Event Expressions (CEE). If logging mechanisms within systems do not conform to standardized formats, systems may convert individual audit records into standardized formats when compiling system-wide audit trails.
None

CHANGES BY AUTHORIZED INDIVIDUALS

organization-defined individuals or roles
organization-defined individuals or roles

organization-defined system components
organization-defined system components

organization-defined selectable event criteria
organization-defined selectable event criteria

organization-defined time thresholds
organization-defined time thresholds
name: AU-12 (3)

statement

Provide and implement the capability for to change the auditing to be performed on based on within .

guidance

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

QUERY PARAMETER AUDITS OF PERSONALLY IDENTIFIABLE INFORMATION

name: AU-12 (4)

statement

Provide and implement the capability for auditing the parameters of user query events for data sets containing personally identifiable information.

guidance

Query parameters are explicit criteria that a user or automated system submits to a system to retrieve data. Auditing of query parameters within systems for datasets that contain personally identifiable information augments an organization's ability to track and understand the access, usage, or sharing of personally identifiable information by authorized personnel.
None

MONITORING FOR INFORMATION DISCLOSURE

organization-defined open source information and/or information sites
organization-defined open source information and/or information sites

organization-defined frequency
organization-defined frequency
name: AU-13

statement

Monitor for evidence of unauthorized disclosure of organizational information.

guidance

Open source information includes, for example, social networking sites.

USE OF AUTOMATED TOOLS

name: AU-13 (1)

statement

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

guidance

Automated mechanisms can include, for example, automated scripts to monitor new posts on selected websites, and commercial services providing notifications and alerts to organizations.
None

REVIEW OF MONITORED SITES

organization-defined frequency
organization-defined frequency
name: AU-13 (2)

statement

Review the open source information sites being monitored .

guidance

None.
None

SESSION AUDIT

name: AU-14

statement

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

guidance

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

SYSTEM START-UP

name: AU-14 (1)

statement

Initiate session audits automatically at system start-up.

guidance

None.
None

CAPTURE AND RECORD CONTENT

name: AU-14 (2)

statement

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

guidance

None.
None

REMOTE VIEWING AND LISTENING

name: AU-14 (3)

statement

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

guidance

None.

ALTERNATE AUDIT CAPABILITY

organization-defined alternate audit functionality
organization-defined alternate audit functionality
name: AU-15

statement

Provide an alternate audit capability in the event of a failure in primary audit capability that implements .

guidance

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

CROSS-ORGANIZATIONAL AUDITING

organization-defined methods
organization-defined methods

organization-defined audit information
organization-defined audit information
name: AU-16

statement

Employ for coordinating among external organizations when audit information is transmitted across organizational boundaries.

guidance

When organizations use systems and/or services of external organizations, the auditing capability necessitates a coordinated approach across organizations. For example, maintaining the identity of individuals that requested specific services across organizational boundaries may often be very difficult, and doing so may prove to have significant performance and privacy ramifications. Therefore, it is often the case that cross-organizational auditing simply captures the identity of individuals issuing requests at the initial system, and subsequent systems record that the requests emanated from authorized individuals.

IDENTITY PRESERVATION

name: AU-16 (1)

statement

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

guidance

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

SHARING OF AUDIT INFORMATION

organization-defined organizations
organization-defined organizations

organization-defined cross-organizational sharing agreements
organization-defined cross-organizational sharing agreements
name: AU-16 (2)

statement

Provide cross-organizational audit information to based on .

guidance

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

ASSESSMENT, AUTHORIZATION, AND MONITORING

ASSESSMENT, AUTHORIZATION, AND MONITORING POLICY AND PROCEDURES

organization-defined personnel or roles
organization-defined personnel or roles

organization-defined senior management official
organization-defined senior management official

organization-defined frequency
organization-defined frequency

organization-defined frequency
organization-defined frequency

name: CA-1

statement

item
name: CA-1a.

Develop, document, and disseminate to :

item
name: CA-1a.1.

A security and privacy assessment, authorization, and monitoring policy that:

item
name: CA-1a.1.(a)

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

item
name: CA-1a.1.(b)

Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and

item
name: CA-1a.2.

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

item
name: CA-1b.

Designate an to manage the security and privacy assessment, authorization, and monitoring policy and procedures;

item
name: CA-1c.

Review and update the current security and privacy assessment, authorization, and monitoring:

item
name: CA-1c.1.

Policy ; and

item

name: CA-1c.2.

Procedures ;

item
name: CA-1d.

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

item
name: CA-1e.

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

guidance

This control addresses the establishment of policy and procedures for the effective implementation of the controls and control enhancements in the CA family. The risk management strategy is an important factor in establishing policy and procedures. Comprehensive policy and procedures help provide security and privacy assurance. Security and privacy program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general security and privacy policy or can be represented by multiple policies reflecting the complex nature of organizations. The procedures can be established for security and privacy programs and for systems, if needed. Procedures describe how policies or controls are implemented and can be directed at the personnel or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. It is important to recognize that restating controls does not constitute an organizational policy or procedure.

References

NIST Special Publication 800-12
NIST Special Publication 800-30
NIST Special Publication 800-39
NIST Special Publication 800-50
NIST Special Publication 800-100

ASSESSMENTS

organization-defined frequency
organization-defined frequency

organization-defined individuals or roles
organization-defined individuals or roles
name: CA-2

statement

item
name: CA-2a.

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

item
name: CA-2a.1.

Security and privacy controls and control enhancements under assessment;

item
name: CA-2a.2.

Assessment procedures to be used to determine control effectiveness; and

item
name: CA-2a.3.

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

item
name: CA-2b.

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

item
name: CA-2c.

Assess the security and privacy controls in the system and its environment of operation to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements;

item
name: CA-2d.

Produce a security and privacy assessment report that document the results of the assessment; and

item
name: CA-2e.

Provide the results of the security and privacy control assessment to .

guidance

Organizations assess security and privacy controls in organizational systems and the environments in which those systems operate as part of initial and ongoing authorizations; FISMA annual assessments; continuous monitoring; and system development life cycle activities. Assessments ensure that organizations meet information security and privacy requirements; identify weaknesses and deficiencies in the development process; provide essential information needed to make risk-based decisions as part of authorization processes; and ensure compliance to vulnerability mitigation procedures. Organizations conduct assessments on the implemented controls from Chapter Three as documented in security plans and privacy plans. Organizations can use other types of assessment activities such as vulnerability scanning and system monitoring to maintain the security and privacy posture of systems during the entire life cycle. Assessment reports document assessment results in sufficient detail as deemed necessary by organizations, to determine the accuracy and completeness of the reports and whether the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting requirements. Assessment results are provided to the individuals or roles appropriate for the types of assessments being conducted. For example, assessments conducted in support of authorization decisions are provided to authorizing officials, senior agency officials for privacy, and/or authorizing official designated representatives. To satisfy annual assessment requirements, organizations can use assessment results from the following sources: initial or ongoing system authorizations; continuous monitoring; or system development life cycle activities. Organizations ensure that assessment results are current, relevant to the determination of control effectiveness, and obtained with the appropriate level of assessor independence. Existing control assessment results can be reused to the extent that the results are still valid and can also be supplemented with additional assessments as needed. After the initial authorizations, organizations assess controls during continuous monitoring. Organizations also establish the frequency for ongoing assessments in accordance with organizational continuous monitoring strategies. External audits including, for example, audits by external entities such as regulatory agencies, are outside the scope of this control.

INDEPENDENT ASSESSORS

name: CA-2 (1)

statement

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

guidance

Independent assessors or assessment teams are individuals or groups conducting impartial assessments of systems. Impartiality implies that assessors are free from any perceived or actual conflicts of interest regarding development, operation, sustainment, or management of the

systems under assessment or the determination of control effectiveness. To achieve impartiality, assessors should not create a mutual or conflicting interest with the organizations where the assessments are being conducted; assess their own work; act as management or employees of the organizations they are serving; or place themselves in positions of advocacy for the organizations acquiring their services. Independent assessments can be obtained from elements within organizations or can be contracted to public or private sector entities outside of organizations. Authorizing officials determine the required level of independence based on the security categories of systems and/or the risk to organizational operations, organizational assets, or individuals. Authorizing officials also determine if the level of assessor independence provides sufficient assurance that the results are sound and can be used to make credible, risk-based decisions. This includes determining whether contracted assessment services have sufficient independence, for example, when system owners are not directly involved in contracting processes or cannot influence the impartiality of assessors conducting assessments. When organizations that own the systems are small or organizational structures require that assessments are conducted by individuals that are in the developmental, operational, or management chain of system owners, independence in assessment processes can be achieved by ensuring that assessment results are carefully reviewed and analyzed by independent teams of experts to validate the completeness, accuracy, integrity, and reliability of the results. Organizations recognize that assessments performed for purposes other than direct support to authorization decisions are, when performed by assessors with sufficient independence, more likely to be useable for such decisions, thereby reducing the need to repeat assessments.
None

SPECIALIZED ASSESSMENTS

organization-defined frequency
organization-defined frequency

organization-defined other forms of assessment
organization-defined other forms of assessment

name: CA-2 (2)

statement

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

guidance

Organizations can conduct specialized assessments including, for example, verification, validation, insider threat assessments, malicious user testing, system monitoring, and other forms of testing. Such assessments can improve readiness by exercising organizational capabilities and indicating current performance levels as a means of focusing actions to improve security and privacy. Organizations conduct these types of specialized assessments in accordance with

applicable laws, Executive Orders, directives, policies, regulations, standards, and guidelines. Authorizing officials approve the assessment methods in coordination with the organizational risk executive function. Organizations can incorporate vulnerabilities uncovered during assessments into vulnerability remediation processes.

EXTERNAL ORGANIZATIONS

organization-defined system
organization-defined system

organization-defined external organization
organization-defined external organization

organization-defined requirements
organization-defined requirements

name: CA-2 (3)

statement

Accept the results of security and privacy control assessments of performed by when the assessment meets .

guidance

Organizations may rely on security and privacy control assessments of organizational systems by other (external) organizations. Using such assessments and reusing existing assessment evidence can significantly decrease the time and resources required for assessments by limiting the amount of independent assessment activities that organizations need to perform. The factors that organizations consider in determining whether to accept assessment results from external organizations can vary. Such factors include, for example, past assessment experiences the organization has had with the organization conducting the assessment; the reputation that the assessing organization has with regard to assessments; the level of detail of supporting assessment evidence provided; and the mandates imposed by applicable laws, Executive Orders, directives, policies, regulations, standards, and guidelines.
None

References

FIPS Publication 199
NIST Special Publication 800-37
NIST Special Publication 800-39
NIST Special Publication 800-53A
NIST Special Publication 800-115
NIST Special Publication 800-137

SYSTEM INTERCONNECTIONS

organization-defined frequency
organization-defined frequency
name: CA-3

statement

item
name: CA-3a.

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

item
name: CA-3b.

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

item
name: CA-3c.

Review and update Interconnection Security Agreements .

guidance

This control applies to dedicated connections between two or more separate systems and does not apply to transitory, user-controlled connections such as email and website browsing. Organizations consider the risks that may be introduced when systems are connected to other systems with different security and privacy requirements and controls, including systems within the same organization and systems external to the organization. Authorizing officials determine the risk associated with system connections and the appropriate controls employed. If interconnecting systems have the same authorizing official, organizations do not need to develop Interconnection Security Agreements. Instead, those organizations can describe the interface characteristics between the interconnecting systems in their respective security and privacy plans. If interconnecting systems have different authorizing officials within the same organization, the organizations can develop Interconnection Security Agreements or they can describe the interface characteristics between the systems in the security and privacy plans for the respective systems. Organizations may also incorporate Interconnection Security Agreement information into formal contracts, especially for interconnections established between federal agencies and nonfederal organizations. Risk considerations also include systems sharing the same networks. As part of the risk assessment of connecting to external systems, organizations consider the number and types of transitive connections that exist when establishing such connections.

UNCLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS

organization-defined unclassified, national security system
organization-defined unclassified, national security system

organization-defined boundary protection device
organization-defined boundary protection device
name: CA-3 (1)

statement

Prohibit the direct connection of an to an external network without the use of .

guidance

Organizations typically do not have control over external networks including the Internet. Approved boundary protection devices including, for example, routers and firewalls. mediate communications and information flows between unclassified national security systems and external networks.
None

CLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS

organization-defined boundary protection device
organization-defined boundary protection device
name: CA-3 (2)

statement

Prohibit the direct connection of a classified, national security system to an external network without the use of .

guidance

Organizations typically do not have control over external networks including the Internet. Approved boundary protection devices including, for example, routers and firewalls, mediate communications and information flows between classified national security systems and external networks. In addition, approved boundary protection devices (typically managed interface/cross-domain systems) provide information flow enforcement from systems to external networks.
None

UNCLASSIFIED NON-NATIONAL SECURITY SYSTEM CONNECTIONS

organization-defined unclassified, non-national security system

organization-defined unclassified, non-national security system

Assignment; organization-defined boundary protection device
Assignment; organization-defined boundary protection device
name: CA-3 (3)

statement

Prohibit the direct connection of an to an external network without the use of .

guidance

Organizations typically do not have control over external networks including the Internet. Approved boundary protection devices including, for example, routers and firewalls mediate communications and information flows between unclassified non-national security systems and external networks.
None

CONNECTIONS TO PUBLIC NETWORKS

organization-defined system
organization-defined system
name: CA-3 (4)

statement

Prohibit the direct connection of an to a public network.

guidance

A public network is any network accessible to the general public including, for example, the Internet and organizational extranets with public access.
None

RESTRICTIONS ON EXTERNAL SYSTEM CONNECTIONS

organization-defined systems
organization-defined systems
name: CA-3 (5)

statement

Employ a deny-all, permit-by-exception policy for allowing to connect to external systems.

guidance

Organizations can constrain system connectivity to external domains by employing a deny-all, permit-by-exception policy known as whitelisting. Organizations determine what exceptions, if any, are acceptable. This control enhancement is applied to a system that is connected to

another system. Alternatively, control enhancement SC-7(5) applies to any type of network communications.

SECONDARY AND TERTIARY CONNECTIONS

name: CA-3 (6)

statement

item
name: CA-3 (6)(a)

Identify secondary and tertiary connections to the interconnected systems; and

item
name: CA-3 (6)(b)

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

guidance

For certain critical systems and applications including, for example, high-value assets, it may be necessary to identify second and third level connections to the interconnected systems. The transparency of the protection measures in place in secondary and tertiary systems connected directly or indirectly to organizational systems is essential in understanding the actual security and privacy risks resulting from those interconnections. Organizational systems can inherit risk from secondary and tertiary systems through those connections and make the organizational systems more susceptible to threats, hazards, and adverse consequences.
None

References
FIPS Publication 199
NIST Special Publication 800-47

SECURITY CERTIFICATION

name: CA-4

statement

Incorporated into CA-2.

PLAN OF ACTION AND MILESTONES

organization-defined frequency
organization-defined frequency

name: CA-5

statement

item
name: CA-5a.

Develop a plan of action and milestones for the system to document the planned remedial actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and

item
name: CA-5b.

Update existing plan of action and milestones based on the findings from control assessments, impact analyses, and continuous monitoring activities.

guidance

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

AUTOMATION SUPPORT FOR ACCURACY AND CURRENCY

name: CA-5 (1)

statement

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

guidance

None.
None

References

NIST Special Publication 800-37

AUTHORIZATION

organization-defined frequency
organization-defined frequency
name: CA-6

statement

item

name: CA-6a.

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

item
name: CA-6b.

Ensure that the authorizing official, before commencing operations:

item
name: CA-6b.1.

Authorizes the system for processing; and

item
name: CA-6b.2.

Authorizes the common controls inherited by the system; and

item
name: CA-6c.

Update the authorizations .

guidance

Authorizations are official management decisions by senior officials to authorize operation of systems (including the controls inherited by those systems) and to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of agreed-upon security and privacy controls. Authorizing officials provide budgetary oversight for organizational systems or assume responsibility for the mission and business operations supported by those systems. The authorization process is a federal responsibility and therefore, authorizing officials must be federal employees. Authorizing officials are responsible and accountable for security and privacy risks associated with the operation and use of organizational systems. Nonfederal organizations may have similar processes to authorize their systems and senior officials that assume the authorization role and associated responsibilities. Organizations conduct ongoing authorizations of systems by implementing continuous monitoring programs. Robust continuous monitoring programs reduce the need for separate reauthorization processes. Through the employment of comprehensive continuous monitoring processes, critical information contained in authorization packages including the security and privacy plans, security and privacy assessment reports, and plans of action and milestones, is updated on an ongoing basis. This provides authorizing officials, system owners, and common control providers with an up-to-date status of the security and privacy state of their systems, controls, and environments of operation. To reduce the cost of reauthorization, authorizing officials use the results of continuous monitoring processes to the maximum extent possible as the basis for rendering reauthorization decisions.

JOINT AUTHORIZATION # SAME ORGANIZATION

name: CA-6 (1)

statement

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

guidance

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

JOINT AUTHORIZATION # DIFFERENT ORGANIZATIONS

name: CA-6 (2)

statement

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

guidance

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

References

NIST Special Publication 800-37
NIST Special Publication 800-137

CONTINUOUS MONITORING

organization-defined metrics
organization-defined metrics

organization-defined frequencies
organization-defined frequencies

organization-defined frequencies
organization-defined frequencies

organization-defined personnel or roles
organization-defined personnel or roles

organization-defined frequency
organization-defined frequency
name: CA-7

statement

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

item
name: CA-7a.

Establishing the following security and privacy metrics to be monitored: ;

item
name: CA-7b.

Establishing for monitoring and for ongoing assessment of security and privacy control effectiveness;

item
name: CA-7c.

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

item
name: CA-7d.

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

item

name: CA-7e.

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

item
name: CA-7f.

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

item
name: CA-7g.

Reporting the security and privacy status of the organization and organizational systems to .

guidance

Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security and privacy to support organizational risk management decisions. The terms continuous and ongoing imply that organizations assess security and privacy controls and associated risks at a frequency sufficient to support risk-based decisions. The results of continuous monitoring generate risk response actions by organizations. When monitoring the effectiveness of controls that have been grouped into capabilities, a root-cause analysis may be needed to determine the specific control that has failed. Continuous monitoring programs also allow organizations to maintain the authorizations of systems and common controls over time in highly dynamic environments of operation with changing mission and business needs, threats, vulnerabilities, and technologies. Having access to security- and privacy-related information on a continuing basis through reports and dashboards gives organizational officials the capability to make more effective and timely risk management decisions, including ongoing authorization decisions. Automation supports more frequent updates to hardware, software, and firmware inventories, authorization packages, and other system information. Effectiveness is further enhanced when continuous monitoring outputs are formatted to provide information that is specific, measurable, actionable, relevant, and timely. Continuous monitoring activities are scaled in accordance with the security categories of systems.

INDEPENDENT ASSESSMENT

name: CA-7 (1)

statement

Employ independent assessors or assessment teams to monitor the security and privacy controls in the system on an ongoing basis.

guidance

Organizations can maximize the value of control assessments during the continuous monitoring process by requiring that assessments be conducted by assessors with appropriate levels of

independence. The level of assessor independence required is based on organizational continuous monitoring strategies. Assessor independence provides a degree of impartiality to the monitoring process. To achieve such impartiality, assessors should not create a mutual or conflicting interest with the organizations where the assessments are being conducted; assess their own work; act as management or employees of the organizations they are serving; or place themselves in advocacy positions for the organizations acquiring their services.
None

TYPES OF ASSESSMENTS

name: CA-7 (2)

statement

Incorporated into CA-2.

TREND ANALYSES

name: CA-7 (3)

statement

Employ trend analyses to determine if security and privacy control implementations, the frequency of continuous monitoring activities, and the types of activities used in the continuous monitoring process need to be modified based on empirical data.

guidance

Trend analyses can include, for example, examining recent threat information regarding the types of threat events that have occurred within the organization or the federal government, success rates of certain types of attacks, emerging vulnerabilities in specific technologies, evolving social engineering techniques, results from multiple control assessments, the effectiveness of configuration settings, and findings from Inspectors General or auditors.
None

RISK MONITORING

name: CA-7 (4)

statement

Ensure risk monitoring is an integral part of the continuous monitoring strategy that includes the following:

item

name: CA-7 (4)(a)

Effectiveness monitoring;

item

name: CA-7 (4)(b)

Compliance monitoring; and

item
name: CA-7 (4)(c)

Change monitoring.

guidance

Effectiveness monitoring determines the ongoing effectiveness of implemented risk response measures. Compliance monitoring verifies that the required risk response measures are implemented. It also verifies that security and privacy requirements are satisfied. Change monitoring identifies changes to organizational systems and environments of operation that may affect security and privacy risk.
None

References
NIST Special Publication 800-37
NIST Special Publication 800-39
NIST Special Publication 800-53A
NIST Special Publication 800-115
NIST Special Publication 800-137

PENETRATION TESTING

organization-defined frequency
organization-defined frequency

organization-defined systems or system components
organization-defined systems or system components
name: CA-8

statement

Conduct penetration testing on .

guidance

Penetration testing is a specialized type of assessment conducted on systems or individual system components to identify vulnerabilities that could be exploited by adversaries. Penetration testing goes beyond automated vulnerability scanning and is most effectively conducted by penetration testing agents and teams with demonstrable skills and experience that, depending on the scope of the penetration testing, include technical expertise in network, operating system, and/or application level security. Penetration testing can be used to either validate vulnerabilities or determine the degree of penetration resistance of systems to adversaries within specified constraints. Such constraints include, for example, time, resources, and skills. Penetration testing attempts to duplicate the actions of adversaries in carrying out attacks

against organizations and provides a more in-depth analysis of security- and privacy-related weaknesses or deficiencies. Organizations can use the results of vulnerability analyses to support penetration testing activities. Penetration testing can be conducted on the hardware, software, or firmware components of a system and can exercise both physical and technical controls. A standard method for penetration testing includes, for example, pretest analysis based on full knowledge of the target system; pretest identification of potential vulnerabilities based on pretest analysis; and testing designed to determine exploitability of identified vulnerabilities. All parties agree to the rules of engagement before commencement of penetration testing scenarios. Organizations correlate the rules of engagement for the penetration tests with the tools, techniques, and procedures that are anticipated to be employed by adversaries carrying out attacks. Risk assessments guide the decisions on the level of independence required for personnel conducting penetration testing.

INDEPENDENT PENETRATION AGENT OR TEAM

name: CA-8 (1)

statement

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

guidance

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

RED TEAM EXERCISES

organization-defined red team exercises
organization-defined red team exercises

name: CA-8 (2)

statement

Employ to simulate attempts by adversaries to compromise organizational systems in accordance with applicable rules of engagement.

guidance

Red team exercises extend the objectives of penetration testing by examining the security and privacy posture of organizations and their ability to implement effective cyber defenses. Red team exercises reflect simulated attempts by adversaries to compromise organizational missions and business functions and provide a comprehensive assessment of the security and

privacy state of systems and organizations. Simulated attempts by adversaries to compromise missions and business functions and the systems that support those missions and functions may include technology-based attacks and social engineering-based attacks. Technology-based attacks include interactions with hardware, software, or firmware components and/or mission and business processes. Social engineering-based attacks include interactions via email, telephone, shoulder surfing, or personal conversations. Red team exercises are most effectively conducted by penetration testing agents and teams with knowledge of and experience with current adversarial tactics, techniques, procedures, and tools. While penetration testing may be primarily laboratory-based testing, organizations can use red team exercises to provide more comprehensive assessments that reflect real-world conditions. Red team exercises can be used to improve security and privacy awareness and training and to assess control effectiveness.
None

FACILITY PENETRATION TESTING

organization-defined frequency
organization-defined frequency
name: CA-8 (3)

statement

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

guidance

None.

INTERNAL SYSTEM CONNECTIONS

organization-defined system components or classes of components
organization-defined system components or classes of components
name: CA-9

statement

item
name: CA-9a.

Authorize internal connections of to the system; and

item
name: CA-9b.

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

guidance

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

COMPLIANCE CHECKS

name: CA-9 (1)

statement

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

guidance

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

References

NIST Special Publication 800-124

CONFIGURATION MANAGEMENT

CONFIGURATION MANAGEMENT POLICY AND PROCEDURES

organization-defined personnel or roles
organization-defined personnel or roles

organization-defined senior management official
organization-defined senior management official

organization-defined frequency
organization-defined frequency

organization-defined frequency
organization-defined frequency

name: CM-1

statement

item

name: CM-1a.

Develop, document, and disseminate to :

item
name: CM-1a.1.

A configuration management policy that:

item
name: CM-1a.1.(a)

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

item
name: CM-1a.1.(b)

Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and

item
name: CM-1a.2.

Procedures to facilitate the implementation of the configuration management policy and the associated configuration management controls;

item
name: CM-1b.

Designate an to manage configuration management policy and procedures;

item
name: CM-1c.

Review and update the current configuration management:

item
name: CM-1c.1.

Policy ; and

item
name: CM-1c.2.

Procedures ;

item
name: CM-1d.

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

item
name: CM-1e.

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

guidance

This control addresses the establishment of policy and procedures for the effective implementation of the controls and control enhancements in the CM family. The risk management strategy is an important factor in establishing policy and procedures. Comprehensive policy and procedures help provide security and privacy assurance. Security and privacy program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general security and privacy policy or can be represented by multiple policies reflecting the complex nature of organizations. The procedures can be established for security and privacy programs and for systems, if needed. Procedures describe how policies or controls are implemented and can be directed at the personnel or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. It is important to recognize that restating controls does not constitute an organizational policy or procedure.

References
NIST Special Publication 800-12
NIST Special Publication 800-30
NIST Special Publication 800-39
NIST Special Publication 800-100

BASELINE CONFIGURATION

organization-defined frequency
organization-defined frequency

Assignment organization-defined circumstances
Assignment organization-defined circumstances
name: CM-2

statement

item
name: CM-2a.

Develop, document, and maintain under configuration control, a current baseline configuration of the system; and

item
name: CM-2b.

Review and update the baseline configuration of the system:

item
name: CM-2b.1.

;

item
name: CM-2b.2.

When required due to ; and

item
name: CM-2b.3.

When system components are installed or upgraded.

guidance

This control establishes baseline configurations for systems and system components including communications and connectivity-related aspects of systems. Baseline configurations are documented, formally reviewed and agreed-upon sets of specifications for systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, and/or changes to systems. Baseline configurations include information about system components, network topology, and the logical placement of those components within the system architecture. Maintaining baseline configurations requires creating new baselines as organizational systems change over time. Baseline configurations of systems reflect the current enterprise architecture.

REVIEWS AND UPDATES

name: CM-2 (1)

statement

Incorporated into CM-2.

AUTOMATION SUPPORT FOR ACCURACY AND CURRENCY

name: CM-2 (2)

statement

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

guidance

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

RETENTION OF PREVIOUS CONFIGURATIONS

organization-defined previous versions of baseline configurations of the system
organization-defined previous versions of baseline configurations of the system
name: CM-2 (3)

statement

Retain to support rollback.

guidance

Retaining previous versions of baseline configurations to support rollback may include, for example, hardware, software, firmware, configuration files, and configuration records.
None

UNAUTHORIZED SOFTWARE

name: CM-2 (4)
CM-7(4)

statement

Incorporated into CM-7(4).

AUTHORIZED SOFTWARE

name: CM-2 (5)
CM-7(5)

statement

Incorporated into CM-7(5).

DEVELOPMENT AND TEST ENVIRONMENTS

name: CM-2 (6)

statement

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

guidance

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

CONFIGURE SYSTEMS AND COMPONENTS FOR HIGH-RISK AREAS

organization-defined systems or system components
organization-defined systems or system components

organization-defined configurations
organization-defined configurations

organization-defined security safeguards
organization-defined security safeguards
name: CM-2 (7)

statement

item
name: CM-2 (7)(a)

Issue with to individuals traveling to locations that the organization deems to be of significant risk; and

item
name: CM-2 (7)(b)

Apply to the components when the individuals return from travel.

guidance

When it is known that systems or system components will be in high-risk areas, additional controls may be implemented to counter the increased threat in such areas. For example,

organizations can take specific actions for notebook computers used by individuals departing on and returning from travel. These actions can include, for example, determining which locations are of concern, defining required configurations for the devices, ensuring that the devices are configured as intended before travel is initiated, and applying specific safeguards to the component after travel is completed. Specially configured notebook computers include, for example, computers with sanitized hard drives, limited applications, and more stringent configuration settings. Specified safeguards applied to mobile devices upon return from travel include, for example, examining the device for signs of physical tampering; and purging and reimaging the hard disk drive. Protecting information residing on mobile devices is covered in the media protection family.
None

References
NIST Special Publication 800-124
NIST Special Publication 800-128

CONFIGURATION CHANGE CONTROL

organization-defined time-period
organization-defined time-period

organization-defined configuration change control element
organization-defined configuration change control element

organization-defined frequency
organization-defined frequency

organization-defined configuration change conditions
organization-defined configuration change conditions
name: CM-3

statement

item
name: CM-3a.

Determine the types of changes to the system that are configuration-controlled;

item
name: CM-3b.

Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security impact analyses;

item
name: CM-3c.

Document configuration change decisions associated with the system;

item
name: CM-3d.

Implement approved configuration-controlled changes to the system;

item
name: CM-3e.

Retain records of configuration-controlled changes to the system for ;

item
name: CM-3f.

Monitor and review activities associated with configuration-controlled changes to the system; and

item
name: CM-3g.

Coordinate and provide oversight for configuration change control activities through that convenes [Selection (one or more): ;].

guidance

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

AUTOMATED DOCUMENTATION, NOTIFICATION, AND PROHIBITION OF CHANGES

organized-defined approval authorities
organized-defined approval authorities

organization-defined time-period
organization-defined time-period

organization-defined personnel
organization-defined personnel
name: CM-3 (1)

statement

Employ automated mechanisms to:

item
name: CM-3 (1)(a)

Document proposed changes to the system;

item
name: CM-3 (1)(b)

Notify of proposed changes to the system and request change approval;

item
name: CM-3 (1)(c)

Highlight proposed changes to the system that have not been approved or disapproved by ;

item
name: CM-3 (1)(d)

Prohibit changes to the system until designated approvals are received;

item
name: CM-3 (1)(e)

Document all changes to the system; and

item
name: CM-3 (1)(f)

Notify when approved changes to the system are completed.

guidance

None.
None

TESTING, VALIDATION, AND DOCUMENTATION OF CHANGES

name: CM-3 (2)

statement

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

guidance

Changes to systems include modifications to hardware, software, or firmware components and configuration settings defined in CM-6. Organizations ensure that testing does not interfere with system operations. Individuals or groups conducting tests understand organizational security and privacy policies and procedures, system security and privacy policies and procedures, and the health, safety, and environmental risks associated with specific facilities or processes. Operational systems may need to be taken off-line, or replicated to the extent feasible, before testing can be conducted. If systems must be taken off-line for testing, the tests are scheduled to occur during planned system outages whenever possible. If the testing cannot be conducted on operational systems, organizations employ compensating controls.
None

AUTOMATED CHANGE IMPLEMENTATION

name: CM-3 (3)

statement

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

guidance

None.
None

SECURITY REPRESENTATIVE

organization-defined information security representative
organization-defined information security representative

organization-defined configuration change control element
organization-defined configuration change control element

name: CM-3 (4)

statement

Require an to be a member of the .

guidance

Information security representatives can include, for example, Senior Agency Information Security Officers, system security officers, or system security managers. Representation

by personnel with information security expertise is important because changes to system configurations can have unintended side effects, some of which may be security-relevant. Detecting such changes early in the process can help avoid unintended, negative consequences that could ultimately affect the security state of organizational systems. The configuration change control element in this control enhancement reflects the change control elements defined by organizations in CM-3.
None

AUTOMATED SECURITY RESPONSE

organization-defined security responses
organization-defined security responses
name: CM-3 (5)

statement

Implement automatically if baseline configurations are changed in an unauthorized manner.

guidance

Security responses include, for example, halting system processing, halting selected system functions, or issuing alerts or notifications to organizational personnel when there is an unauthorized modification of a configuration item.
None

CRYPTOGRAPHY MANAGEMENT

organization-defined security safeguards
organization-defined security safeguards
name: CM-3 (6)

statement

Ensure that cryptographic mechanisms used to provide are under configuration management.

guidance

Regardless of the cryptographic means employed, organizations ensure that there are processes and procedures in place to manage those means. For example, if devices use certificates for identification and authentication, a process is implemented to address the expiration of those certificates.

References

NIST Special Publication 800-124
NIST Special Publication 800-128

SECURITY AND PRIVACY IMPACT ANALYSES

name: CM-4

statement

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

guidance

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

SEPARATE TEST ENVIRONMENTS

name: CM-4 (1)

statement

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

guidance

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

VERIFICATION OF SECURITY AND PRIVACY FUNCTIONS

name: CM-4 (2)

statement

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

guidance

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

References

NIST Special Publication 800-128

ACCESS RESTRICTIONS FOR CHANGE

name: CM-5

statement

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

guidance

Any changes to the hardware, software, and/or firmware components of systems can potentially have significant effects on the overall security of the systems. Therefore, organizations permit only qualified and authorized individuals to access systems for purposes of initiating changes, including upgrades and modifications. Access restrictions for change also include software libraries. Access restrictions include, for example, physical and logical access controls (see AC-3 and PE-3), workflow automation, media libraries, abstract layers (i.e., changes implemented into external interfaces rather than directly into systems), and change windows (i.e., changes occur only during specified times).

AUTOMATED ACCESS ENFORCEMENT AND AUDITING

name: CM-5 (1)

statement

item

name: CM-5 (1)(a)

Enforce access restrictions; and

item

name: CM-5 (1)(b)

Generate audit records of the enforcement actions.

guidance

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

REVIEW SYSTEM CHANGES

organization-defined frequency
organization-defined frequency

organization-defined circumstances
organization-defined circumstances
name: CM-5 (2)

statement

Review system changes and to determine whether unauthorized changes have occurred.

guidance

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

SIGNED COMPONENTS

organization-defined software and firmware components
organization-defined software and firmware components
name: CM-5 (3)

statement

Prevent the installation of without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

guidance

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

DUAL AUTHORIZATION

organization-defined system components and system-level information
organization-defined system components and system-level information
name: CM-5 (4)

statement

Enforce dual authorization for implementing changes to .

guidance

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

PRIVILEGE LIMITATION FOR PRODUCTION AND OPERATION

organization-defined frequency
organization-defined frequency
name: CM-5 (5)

statement

item
name: CM-5 (5)(a)

Limit privileges to change system components and system-related information within a production or operational environment; and

item
name: CM-5 (5)(b)

Review and reevaluate privileges .

guidance

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

LIMIT LIBRARY PRIVILEGES

name: CM-5 (6)

statement

Limit privileges to change software resident within software libraries.

guidance

Software libraries include privileged programs.

AUTOMATIC IMPLEMENTATION OF SECURITY SAFEGUARDS

name: CM-5 (7)

statement

Incorporated into SI-7.

References

FIPS Publication 140-2

CONFIGURATION SETTINGS

organization-defined common secure configurations
organization-defined common secure configurations

organization-defined system components
organization-defined system components

organization-defined operational requirements
organization-defined operational requirements

name: CM-6

statement

item

name: CM-6a.

Establish and document configuration settings for components employed within the system using that reflect the most restrictive mode consistent with operational requirements;

item

name: CM-6b.

Implement the configuration settings;

item

name: CM-6c.

Identify, document, and approve any deviations from established configuration settings for based on ; and

item

name: CM-6d.

Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

guidance

Configuration settings are the parameters that can be changed in hardware, software, or firmware components of the system that affect the security posture or functionality of the system. Information technology products for which security-related configuration settings can be defined include, for example, mainframe computers, servers, workstations, input/output devices, network devices, operating systems, and applications. Security-related parameters are those parameters impacting the security state of systems including the parameters required to satisfy other security control requirements. Security-related parameters include, for example, registry settings; account, file, directory permission settings; and settings for functions, ports, protocols, and remote connections. Organizations establish organization-wide configuration settings and subsequently derive specific configuration settings for systems. The established settings become part of the systems configuration baseline. Common secure configurations (also referred to as security configuration checklists, lockdown and hardening guides, security reference guides, security technical implementation guides) provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for specific information technology platforms/products and instructions for configuring those system components to meet operational requirements. Common secure configurations can be developed by a variety of organizations including, for example, information technology product developers, manufacturers, vendors, consortia, academia, industry, federal agencies, and other organizations in the public and private sectors. Implementation of a specific common secure configuration may be mandated at the organizational or mission/business process level or may be mandated at a higher level including, for example, by a regulatory agency. Common secure configurations include the United States Government Configuration Baseline (USGCB) which affects the implementation of CM-6 and other controls such as AC-19 and CM-7. The Security Content Automation Protocol (SCAP) and the defined standards within the protocol provide an effective method to uniquely identify, track, and control configuration settings.

AUTOMATED MANAGEMENT, APPLICATION, AND VERIFICATION

organization-defined system components
organization-defined system components
name: CM-6 (1)

statement

Employ automated mechanisms to centrally manage, apply, and verify configuration settings for .

guidance

RESPOND TO UNAUTHORIZED CHANGES

organization-defined security safeguards
organization-defined security safeguards

organization-defined configuration settings
organization-defined configuration settings
name: CM-6 (2)

statement

Employ to respond to unauthorized changes to .

guidance

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

UNAUTHORIZED CHANGE DETECTION

name: CM-6 (3)

statement

Incorporated into SI-7.

CONFORMANCE DEMONSTRATION

name: CM-6 (4)

statement

Incorporated into CM-4.

References

NIST Special Publication 800-70
NIST Special Publication 800-128

LEAST FUNCTIONALITY

organization-defined prohibited or restricted functions, ports, protocols, and/or services
organization-defined prohibited or restricted functions, ports, protocols, and/or services
name: CM-7

statement

item
name: CM-7a.

Configure the system to provide only essential capabilities; and

item
name: CM-7b.

Prohibit or restrict the use of the following functions, ports, protocols, and/or services: .

guidance

Systems provide a wide variety of functions and services. Some of the functions and services routinely provided by default, may not be necessary to support essential organizational missions, functions, or operations. Additionally, it is sometimes convenient to provide multiple services from a single system component, but doing so increases risk over limiting the services provided by that single component. Where feasible, organizations limit component functionality to a single function per component. Organizations review functions and services provided by systems or components of systems, to determine which functions and services are candidates for elimination. Organizations consider disabling unused or unnecessary physical and logical ports and protocols to prevent unauthorized connection of devices, transfer of information, and tunneling. Organizations employ network scanning tools, intrusion detection and prevention systems, and end-point protection technologies such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, protocols, ports, and services. Related Controls: AC-3, AC-4, CM-2, CM-5, CM-11, RA-5, SA-4, SA-5, SA-9, SA-15, SC-7, SC-37. SI-4.

PERIODIC REVIEW

organization-defined frequency
organization-defined frequency

organization-defined functions, ports, protocols, and services within the system deemed to be unnecessary and/or nonsecure
organization-defined functions, ports, protocols, and services within the system deemed to be unnecessary and/or nonsecure
name: CM-7 (1)

statement

item
name: CM-7 (1)(a)

Review the system to identify unnecessary and/or nonsecure functions, ports, protocols, and services; and

item
name: CM-7 (1)(b)

Disable .

guidance

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

PREVENT PROGRAM EXECUTION

organization-defined policies regarding software program usage and restrictions
organization-defined policies regarding software program usage and restrictions
name: CM-7 (2)

statement

Prevent program execution in accordance with [Selection (one or more): ; rules authorizing the terms and conditions of software program usage].

guidance

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

REGISTRATION COMPLIANCE

organization-defined registration requirements for functions, ports, protocols, and services
organization-defined registration requirements for functions, ports, protocols, and services
name: CM-7 (3)

statement

Ensure compliance with .

guidance

Organizations use the registration process to manage, track, and provide oversight for systems and implemented functions, ports, protocols, and services.
None

UNAUTHORIZED SOFTWARE # BLACKLISTING

organization-defined software programs not authorized to execute on the system
organization-defined software programs not authorized to execute on the system

organization-defined frequency
organization-defined frequency
name: CM-7 (4)

statement

item
name: CM-7 (4)(a)

Identify ;

item
name: CM-7 (4)(b)

Employ an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the system; and

item
name: CM-7 (4)(c)

Review and update the list of unauthorized software programs .

guidance

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

AUTHORIZED SOFTWARE # WHITELISTING

organization-defined software programs authorized to execute on the system
organization-defined software programs authorized to execute on the system

organization-defined frequency
organization-defined frequency
name: CM-7 (5)

statement

item
name: CM-7 (5)(a)

Identify ;

item
name: CM-7 (5)(b)

Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system; and

item
name: CM-7 (5)(c)

Review and update the list of authorized software programs .

guidance

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

References
FIPS Publication 140-2

SYSTEM COMPONENT INVENTORY

organization-defined information deemed necessary to achieve effective system component accountability
organization-defined information deemed necessary to achieve effective system component accountability

organization-defined frequency
organization-defined frequency
name: CM-8

statement

item
name: CM-8a.

Develop and document an inventory of system components that:

item
name: CM-8a.1.

Accurately reflects the current system;

item
name: CM-8a.2.

Includes all components within the authorization boundary of the system;

item
name: CM-8a.3.

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

item
name: CM-8a.4.

Includes ; and

item
name: CM-8b.

Review and update the system component inventory .

guidance

System components are discrete identifiable information technology assets that represent a building block of a system and include hardware, software, firmware, and virtual machines. Organizations may choose to implement centralized system component inventories that include components from all organizational systems. In such situations, organizations ensure that the inventories include system-specific information required for proper component accountability. Information necessary for effective accountability of system components includes, for example, hardware inventory specifications; software license information; software component owners; version numbers; and for networked components or devices, the machine names and network addresses. Inventory specifications include, for example, manufacturer; device type; model; serial number; and physical location.

UPDATES DURING INSTALLATION AND REMOVAL

name: CM-8 (1)

statement

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

guidance

None.
None

AUTOMATED MAINTENANCE

name: CM-8 (2)

statement

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

guidance

Organizations maintain system inventories to the extent feasible. Virtual machines, for example, can be difficult to monitor because such machines are not visible to the network when not in use. In such cases, organizations maintain as up-to-date, complete, and accurate an inventory as is deemed reasonable. This control enhancement can be satisfied by the implementation of CM-2 (2) for organizations that choose to combine system component inventory and baseline configuration activities.
None

AUTOMATED UNAUTHORIZED COMPONENT DETECTION

organization-defined frequency
organization-defined frequency

organization-defined personnel or roles
organization-defined personnel or roles
name: CM-8 (3)

statement

item
name: CM-8 (3)(a)

Employ automated mechanisms to detect the presence of unauthorized hardware, software, and firmware components within the system; and

item
name: CM-8 (3)(b)

Take the following actions when unauthorized components are detected: [Selection (one or more): disable network access by such components; isolate the components; notify].

guidance

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

ACCOUNTABILITY INFORMATION

name: CM-8 (4)

statement

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

guidance

Identifying individuals who are both responsible and accountable for administering system components helps to ensure that the assigned components are properly administered and organizations can contact those individuals if some action is required, for example, the component is determined to be the source of a breach; the component needs to be recalled or replaced; or the component needs to be relocated.

None

NO DUPLICATE ACCOUNTING OF COMPONENTS

name: CM-8 (5)

statement

item

name: CM-8 (5)(a)

Verify that all components within the authorization boundary of the system are not duplicated in other system component inventories; or

item

name: CM-8 (5)(b)

If a centralized component inventory is used, verify components are not assigned to multiple systems.

guidance

This control enhancement addresses the potential problem of duplicate accounting of system components in large or complex interconnected systems.

None

ASSESSED CONFIGURATIONS AND APPROVED DEVIATIONS

name: CM-8 (6)

statement

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

guidance

This control enhancement focuses on configuration settings established by organizations for system components, the specific components that have been assessed to determine compliance with the required configuration settings, and any approved deviations from established configuration settings.
None

CENTRALIZED REPOSITORY

name: CM-8 (7)

statement

Provide a centralized repository for the inventory of system components.

guidance

Organizations may choose to implement centralized system component inventories that include components from all organizational systems. Centralized repositories of system component inventories provide opportunities for efficiencies in accounting for organizational hardware, software, and firmware assets. Such repositories may also help organizations rapidly identify the location and responsible individuals of system components that have been compromised, breached, or are otherwise in need of mitigation actions. Organizations ensure that the resulting centralized inventories include system-specific information required for proper component accountability.
None

AUTOMATED LOCATION TRACKING

name: CM-8 (8)

statement

Employ automated mechanisms to support tracking of system components by geographic location.

guidance

The use of automated mechanisms to track the location of system components can increase the accuracy of component inventories. Such capability may also help organizations rapidly identify the location and responsible individuals of system components that have been compromised, breached, or are otherwise in need of mitigation actions.
None

ASSIGNMENT OF COMPONENTS TO SYSTEMS

organization-defined acquired system components
organization-defined acquired system components

organization-defined personnel or roles
organization-defined personnel or roles
name: CM-8 (9)

statement

item
name: CM-8 (9)(a)

Assign to a system; and

item
name: CM-8 (9)(b)

Receive an acknowledgement from of this assignment.

guidance

Organizations determine the types of system components that are subject to this control enhancement.
None

DATA ACTION MAPPING

name: CM-8 (10)

statement

Develop and document a system map of data actions that process personally identifiable information.

guidance

Data actions are system operations that process personally identifiable information. Such processing encompasses the full information life cycle which includes collection, generation, transformation, use, disclosure, retention, disposal. Creating a system map of data actions supports a privacy risk assessment. The development of this map may necessitate coordination between the privacy and security programs regarding the covered data actions, the system components, and the definition of the authorization boundary.

References

CONFIGURATION MANAGEMENT PLAN

organization-defined personnel or roles
organization-defined personnel or roles
name: CM-9

statement

Develop, document, and implement a configuration management plan for the system that:

item
name: CM-9a.

Addresses roles, responsibilities, and configuration management processes and procedures;

item
name: CM-9b.

Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;

item
name: CM-9c.

Defines the configuration items for the system and places the configuration items under configuration management;

item
name: CM-9d.

Is reviewed and approved by ; and

item
name: CM-9e.

Protects the configuration management plan from unauthorized disclosure and modification.

guidance

Configuration management plans satisfy the requirements in configuration management policies while being tailored to individual systems. Such plans define processes and procedures for how configuration management is used to support system development life cycle activities. Configuration management plans are typically developed during the development and acquisition phase of the system development life cycle. The plans describe how to move changes through change management processes, how to update configuration settings and baselines, how to maintain system component inventories, how to control development, test, and operational environments, and how to develop, release, and update key documents. Organizations can employ templates to help ensure consistent and timely development and implementation

of configuration management plans. Such templates can represent a master configuration management plan for the organization with subsets of the plan implemented on a system by system basis. Configuration management approval processes include designation of key management stakeholders responsible for reviewing and approving proposed changes to systems, and personnel that conduct security impact analyses prior to the implementation of changes to the systems. Configuration items are the system components (i.e., hardware, software, firmware, and documentation) to be configuration-managed. As systems continue through the system development life cycle, new configuration items may be identified and some existing configuration items may no longer need to be under configuration control.

ASSIGNMENT OF RESPONSIBILITY

name: CM-9 (1)

statement

Assign responsibility for developing the configuration management process to organizational personnel that are not directly involved in system development.

guidance

In the absence of dedicated configuration management teams assigned within organizations, system developers may be tasked to develop configuration management processes using personnel who are not directly involved in system development or integration. This separation of duties ensures that organizations establish and maintain a sufficient degree of independence between the system development and integration processes and configuration management processes to facilitate quality control and more effective oversight.
None

References

NIST Special Publication 800-128

SOFTWARE USAGE RESTRICTIONS

name: CM-10

statement

item

name: CM-10a.

Use software and associated documentation in accordance with contract agreements and copyright laws;

item

name: CM-10b.

Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and

item
name: CM-10c.

Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

guidance

Software license tracking can be accomplished by manual methods or automated methods depending on organizational needs.

OPEN SOURCE SOFTWARE

organization-defined restrictions
organization-defined restrictions
name: CM-10 (1)

statement

Establish the following restrictions on the use of open source software: .

guidance

Open source software refers to software that is available in source code form. Certain software rights normally reserved for copyright holders are routinely provided under software license agreements that permit individuals to study, change, and improve the software. From a security perspective, the major advantage of open source software is that it provides organizations with the ability to examine the source code. However, there are also various licensing issues associated with open source software including, for example, the constraints on derivative use of such software.

USER-INSTALLED SOFTWARE

organization-defined policies
organization-defined policies

organization-defined methods
organization-defined methods

organization-defined frequency
organization-defined frequency
name: CM-11

statement

item
name: CM-11a.

Establish governing the installation of software by users;

item
name: CM-11b.

Enforce software installation policies through the following methods: ; and

item
name: CM-11c.

Monitor policy compliance at .

guidance

If provided the necessary privileges, users have the ability to install software in organizational systems. To maintain control over the types of software installed, organizations identify permitted and prohibited actions regarding software installation. Permitted software installations may include, for example, updates and security patches to existing software and downloading applications from organization-approved #app stores.# Prohibited software installations may include, for example, software with unknown or suspect pedigrees or software that organizations consider potentially malicious. The policies organizations select governing user-installed software may be organization-developed or provided by some external entity. Policy enforcement methods include procedural methods, automated methods, or both.

ALERTS FOR UNAUTHORIZED INSTALLATIONS

name: CM-11 (1)
CM-8(3)

statement

Incorporated into CM-8(3).

SOFTWARE INSTALLATION WITH PRIVILEGED STATUS

name: CM-11 (2)

statement

Allow user installation of software only with explicit privileged status.

guidance

Privileged status can be obtained, for example, by serving in the role of system administrator.

INFORMATION LOCATION

organization-defined information
organization-defined information
name: CM-12

statement

item
name: CM-12a.

Identify the location of and the specific system components on which the information resides;

item
name: CM-12b.

Identify and document the users who have access to the system and system components where the information resides; and

item
name: CM-12c.

Document changes to the location (i.e., system or system components) where the information resides.

guidance

This control addresses the need to understand where information is being processed and stored and is typically applied with respect to Controlled Unclassified Information (CUI). The National Archives and Records Administration defines the types of information that are categorized as CUI. Information location includes identifying where specific information types and associated information reside in the system components that compose organizational systems; and how information is being processed so that information flow can be understood and adequate protection and policy management provided for such information and system components.

AUTOMATED TOOLS TO SUPPORT INFORMATION LOCATION

organization-defined information by information type
organization-defined information by information type

organization-defined system components
organization-defined system components
name: CM-12 (1)

statement

Use automated tools to identify on to ensure adequate security and privacy controls are in place to protect organizational information and individual privacy.

guidance

This control enhancement gives organizations the capability to check systems and selected system components for types of information to confirm such information resides on the component and to ensure that the required protection measures are in place for that component.
None

References
FIPS Publication 199

CONTINGENCY PLANNING

CONTINGENCY PLANNING POLICY AND PROCEDURES

organization-defined personnel or roles
organization-defined personnel or roles

organization-defined senior management official
organization-defined senior management official

organization-defined frequency
organization-defined frequency

organization-defined frequency
organization-defined frequency
name: CP-1

statement

item
name: CP-1a.

Develop, document, and disseminate to :

item
name: CP-1a.1.

A contingency planning policy that:

item
name: CP-1a.1.(a)

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

item
name: CP-1a.1.(b)

Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and

item
name: CP-1a.2.

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

item
name: CP-1b.

Designate an to manage the contingency planning policy and procedures;

item
name: CP-1c.

Review and update the current contingency planning:

item
name: CP-1c.1.

Policy ; and

item
name: CP-1c.2.

Procedures ;

item
name: CP-1d.

Ensure that the contingency planning procedures implement the contingency planning policy and controls; and

item
name: CP-1e.

Develop, document, and implement remediation actions for violations of the contingency planning policy.

guidance

This control addresses the establishment of policy and procedures for the effective implementation of the controls and control enhancements in the CP family. The risk management strategy is an important factor in establishing policy and procedures. Comprehensive policy and procedures help provide security and privacy assurance. Security and privacy program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general security and privacy policy or can be represented by multiple policies reflecting the complex nature of organizations. The procedures can be established for security and privacy programs and for systems, if needed. Procedures describe how policies or controls are implemented and can be directed at the personnel or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. It is important to recognize that restating controls does not constitute an organizational policy or procedure.

References

NIST Special Publication 800-12
NIST Special Publication 800-30
NIST Special Publication 800-34
NIST Special Publication 800-39
NIST Special Publication 800-100

CONTINGENCY PLAN

organization-defined personnel or roles
organization-defined personnel or roles

organization-defined key contingency personnel (identified by name and/or by role) and organizational elements
organization-defined key contingency personnel (identified by name and/or by role) and organizational elements

organization-defined frequency
organization-defined frequency

organization-defined key contingency personnel (identified by name and/or by role) and organizational elements
organization-defined key contingency personnel (identified by name and/or by role) and organizational elements
name: CP-2

statement

item

name: CP-2a.

Develop a contingency plan for the system that:

item
name: CP-2a.1.

Identifies essential missions and business functions and associated contingency requirements;

item
name: CP-2a.2.

Provides recovery objectives, restoration priorities, and metrics;

item
name: CP-2a.3.

Addresses contingency roles, responsibilities, assigned individuals with contact information;

item
name: CP-2a.4.

Addresses maintaining essential missions and business functions despite a system disruption, compromise, or failure;

item
name: CP-2a.5.

Addresses eventual, full system restoration without deterioration of the security and privacy controls originally planned and implemented; and

item
name: CP-2a.6.

Is reviewed and approved by ;

item
name: CP-2b.

Distributes copies of the contingency plan to ;

item
name: CP-2c.

Coordinates contingency planning activities with incident handling activities;

item
name: CP-2d.

Reviews the contingency plan for the system ;

item

name: CP-2e.

Updates the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;

item
name: CP-2f.

Communicates contingency plan changes to ; and

item
name: CP-2g.

Protects the contingency plan from unauthorized disclosure and modification.

guidance

Contingency planning for systems is part of an overall organizational program for achieving continuity of operations for mission/business functions. Contingency planning addresses system restoration and implementation of alternative mission or business processes when systems are compromised or breached. The effectiveness of contingency planning is maximized by considering such planning throughout the system development life cycle. Performing contingency planning on hardware, software, and firmware development can be an effective means of achieving system resiliency. Contingency plans reflect the degree of restoration required for organizational systems since not all systems need to fully recover to achieve the level of continuity of operations desired. System recovery objectives reflect applicable laws, Executive Orders, directives, policies, standards, regulations, and guidelines. In addition to availability, contingency plans address other security-related events resulting in a reduction in mission or business effectiveness, such as malicious attacks compromising the confidentiality or integrity of systems. Actions addressed in contingency plans include, for example, orderly and graceful degradation, system shutdown, fallback to a manual mode, alternate information flows, and operating in modes reserved for when systems are under attack. By coordinating contingency planning with incident handling activities, organizations can ensure that the necessary planning activities are in place and activated in the event of a security incident.

COORDINATE WITH RELATED PLANS

name: CP-2 (1)

statement

Coordinate contingency plan development with organizational elements responsible for related plans.

guidance

Plans related to contingency plans for organizational systems include, for example, Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis

Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, Insider Threat Implementation Plan, and Occupant Emergency Plans.
None

CAPACITY PLANNING

name: CP-2 (2)

statement

Conduct capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.

guidance

Capacity planning is needed because different types of threats can result in a reduction of the available processing, telecommunications, and support services intended to support the organizational missions and business functions. Organizations need to anticipate degraded operations during contingency operations and factor such degradation into capacity planning. With respect to capacity planning, environmental support refers to any environmental support factor for which the organization determines that it needs to provide support in a contingency situation, even if in a degraded state. As always, such determinations are based on an assessment of risk, system categorization (impact level), and organizational risk tolerance.

RESUME ESSENTIAL MISSIONS AND BUSINESS FUNCTIONS

organization-defined time-period
organization-defined time-period

name: CP-2 (3)

statement

Plan for the resumption of essential missions and business functions within of contingency plan activation.

guidance

Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. The time-period for resumption of essential missions and business functions may be dependent on the severity and extent of the disruptions to the system and its supporting infrastructure.
None

RESUME ALL MISSIONS AND BUSINESS FUNCTIONS

organization-defined time-period
organization-defined time-period

name: CP-2 (4)

statement

Plan for the resumption of all missions and business functions within of contingency plan activation.

guidance

Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. The time-period for resumption of missions and business functions may be dependent on the severity and extent of disruptions to the system and its supporting infrastructure.
None

CONTINUE ESSENTIAL MISSIONS AND BUSINESS FUNCTIONS

name: CP-2 (5)

statement

Plan for the continuance of essential missions and business functions with little or no loss of operational continuity and sustains that continuity until full system restoration at primary processing and/or storage sites.

guidance

Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. Primary processing and/or storage sites defined by organizations as part of contingency planning may change depending on the circumstances associated with the contingency.
None

ALTERNATE PROCESSING AND STORAGE SITE

name: CP-2 (6)

statement

Plan for the transfer of essential missions and business functions to alternate processing and/or storage sites with little or no loss of operational continuity and sustain that continuity through system restoration to primary processing and/or storage sites.

guidance

Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. Primary processing and/or storage sites defined by

organizations as part of contingency planning may change depending on the circumstances associated with the contingency.
None

COORDINATE WITH EXTERNAL SERVICE PROVIDERS

name: CP-2 (7)

statement

Coordinate the contingency plan with the contingency plans of external service providers to ensure that contingency requirements can be satisfied.

guidance

When the capability of an organization to successfully carry out its core missions and business functions is dependent on external service providers, developing a timely and comprehensive contingency plan may become more challenging. In this situation, organizations coordinate contingency planning activities with the external entities to ensure that the individual plans reflect the overall contingency needs of the organization.

IDENTIFY CRITICAL ASSETS

name: CP-2 (8)

statement

Identify critical system assets supporting essential missions and business functions.

guidance

Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational criticality analysis or business continuity planning including, for example, as part of business impact analyses. Organizations identify critical system assets so additional safeguards and countermeasures can be employed (beyond those safeguards and countermeasures routinely implemented) to help ensure that organizational missions/business functions can continue to be conducted during contingency operations. The identification of critical information assets also facilitates the prioritization of organizational resources. Critical system assets include both technical and operational aspects. Technical aspects include, for example, information technology services, system components, information technology products, and mechanisms. Operational aspects include, for example, procedures (manually executed operations) and personnel (individuals operating technical safeguards and/or executing manual procedures). Organizational program protection plans can aid in identifying critical assets.

References

NIST Special Publication 800-34

CONTINGENCY TRAINING

organization-defined time-period
organization-defined time-period

organization-defined frequency
organization-defined frequency
name: CP-3

statement

Provide contingency training to system users consistent with assigned roles and responsibilities:

item
name: CP-3a.

Within of assuming a contingency role or responsibility;

item
name: CP-3b.

When required by system changes; and

item
name: CP-3c.

thereafter.

guidance

Contingency training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail is included in such training. For example, regular users may only need to know when and where to report for duty during contingency operations and if normal duties are affected; system administrators may require additional training on how to set up systems at alternate processing and storage sites; and managers/senior leaders may receive more specific training on how to conduct mission-essential functions in designated off-site locations and how to establish communications with other governmental entities for purposes of coordination on contingency-related activities. Training for contingency roles/responsibilities reflects the specific continuity requirements in the contingency plan.

SIMULATED EVENTS
name: CP-3 (1)

statement

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

guidance

None.
None

AUTOMATED TRAINING ENVIRONMENTS

name: CP-3 (2)

statement

Employ automated mechanisms to provide a more thorough and realistic contingency training environment.

guidance

None.
None

References

NIST Special Publication 800-50

CONTINGENCY PLAN TESTING

organization-defined frequency
organization-defined frequency

organization-defined tests
organization-defined tests

name: CP-4

statement

item

name: CP-4a.

Test the contingency plan for the system using to determine the effectiveness of the plan and the organizational readiness to execute the plan;

item

name: CP-4b.

Review the contingency plan test results; and

item

name: CP-4c.

Initiate corrective actions, if needed.

guidance

Methods for testing contingency plans to determine the effectiveness of the plans and to identify potential weaknesses in the plans include, for example, walk-through and tabletop exercises, checklists, simulations (parallel, full interrupt), and comprehensive exercises. Organizations conduct testing based on the continuity requirements in contingency plans and include a determination of the effects on organizational operations, assets, and individuals arising due to contingency operations. Organizations have flexibility and discretion in the breadth, depth, and timelines of corrective actions.

COORDINATE WITH RELATED PLANS

name: CP-4 (1)

statement

Coordinate contingency plan testing with organizational elements responsible for related plans.

guidance

Plans related to contingency plans for organizational systems include, for example, business continuity plans, disaster recovery plans, continuity of operations plans, crisis communications plans, critical infrastructure plans, cyber incident response plans, and occupant emergency plans. This control enhancement does not require organizations to create organizational elements to handle related plans or to align such elements with specific plans. It does require, however, that if such organizational elements are responsible for related plans, organizations should coordinate with those elements.

ALTERNATE PROCESSING SITE

name: CP-4 (2)

statement

Test the contingency plan at the alternate processing site:

item
name: CP-4 (2)(a)

To familiarize contingency personnel with the facility and available resources; and

item
name: CP-4 (2)(b)

To evaluate the capabilities of the alternate processing site to support contingency operations.

guidance

None.

AUTOMATED TESTING

name: CP-4 (3)

statement

Employ automated mechanisms to more thoroughly and effectively test the contingency plan.

guidance

Automated mechanisms facilitate more thorough and effective testing of contingency plans. This occurs by providing more complete coverage of contingency issues; by selecting more realistic test scenarios and environments; and by effectively stressing the system and supported missions and business operations.
None

FULL RECOVERY AND RECONSTITUTION

name: CP-4 (4)

statement

Include a full recovery and reconstitution of the system to a known state as part of contingency plan testing.

guidance

None.

References

FIPS Publication 199
NIST Special Publication 800-34
NIST Special Publication 800-84

CONTINGENCY PLAN UPDATE

name: CP-5

statement

Incorporated into CP-2.

ALTERNATE STORAGE SITE

name: CP-6

statement

item

name: CP-6a.

Establish an alternate storage site including necessary agreements to permit the storage and retrieval of system backup information; and

item
name: CP-6b.

Ensure that the alternate storage site provides security controls equivalent to that of the primary site.

guidance

Alternate storage sites are sites that are geographically distinct from primary storage sites. An alternate storage site maintains duplicate copies of information and data if the primary storage site is not available. Items covered by alternate storage site agreements include, for example, environmental conditions at alternate sites, access rules, physical and environmental protection requirements, and coordination of delivery/retrieval of backup media. Alternate storage sites reflect the requirements in contingency plans so that organizations can maintain essential missions and business functions despite disruption, compromise, or failure in organizational systems.

SEPARATION FROM PRIMARY SITE

name: CP-6 (1)

statement

Identify an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.

guidance

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

RECOVERY TIME AND RECOVERY POINT OBJECTIVES

name: CP-6 (2)

statement

Configure the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.

guidance

None.
None

ACCESSIBILITY

name: CP-6 (3)

statement

Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

guidance

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

References

NIST Special Publication 800-34

ALTERNATE PROCESSING SITE

organization-defined system operations
organization-defined system operations

organization-defined time-period consistent with recovery time and recovery point objectives
organization-defined time-period consistent with recovery time and recovery point objectives
name: CP-7

statement

item
name: CP-7a.

Establish an alternate processing site including necessary agreements to permit the transfer and resumption of for essential missions and business functions within when the primary processing capabilities are unavailable;

item
name: CP-7b.

Make available at the alternate processing site, the equipment and supplies required to transfer and resume operations or put contracts in place to support delivery to the site within the organization-defined time-period for transfer and resumption; and

item
name: CP-7c.

Provide information security and privacy safeguards at the alternate processing site that are equivalent to those at the primary site.

guidance

Alternate processing sites are sites that are geographically distinct from primary processing sites. An alternate processing site provides processing capability if the primary processing site is not available. Geographically distributed architectures may also be considered as alternate processing sites. Safeguards that are covered by alternate processing site agreements include, for example, environmental conditions at alternate sites; access rules; physical and environmental protection requirements; and the coordination for the transfer and assignment of personnel. Requirements are specifically allocated to alternate processing sites that reflect the requirements in contingency plans to maintain essential missions and business functions despite disruption, compromise, or failure in organizational systems.

SEPARATION FROM PRIMARY SITE

name: CP-7 (1)

statement

Identify an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.

guidance

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

ACCESSIBILITY

name: CP-7 (2)

statement

Identify potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

guidance

Area-wide disruptions refer to those types of disruptions that are broad in geographic scope with such determinations made by organizations based on organizational assessments of risk.

PRIORITY OF SERVICE

name: CP-7 (3)

statement

Develop alternate processing site agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives).

guidance

Priority-of-service agreements refer to negotiated agreements with service providers that ensure that organizations receive priority treatment consistent with their availability requirements and the availability of information resources at the alternate processing site.
None

PREPARATION FOR USE

name: CP-7 (4)

statement

Prepare the alternate processing site so that the site is ready to be used as the operational site supporting essential missions and business functions.

guidance

Site preparation includes, for example, establishing configuration settings for system components at the alternate processing site consistent with the requirements for such settings at the primary site and ensuring that essential supplies and other logistical considerations are in place.

EQUIVALENT INFORMATION SECURITY SAFEGUARDS

name: CP-7 (5)

statement

Incorporated into CP-7.

INABILITY TO RETURN TO PRIMARY SITE

name: CP-7 (6)

statement

Plan and prepare for circumstances that preclude returning to the primary processing site.

guidance

None.
None

References

NIST Special Publication 800-34

TELECOMMUNICATIONS SERVICES

organization-defined system operations
organization-defined system operations

organization-defined time-period

organization-defined time-period
name: CP-8

statement

Establish alternate telecommunications services including necessary agreements to permit the resumption of for essential missions and business functions within when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

guidance

This control applies to telecommunications services (data and voice) for primary and alternate processing and storage sites. Alternate telecommunications services reflect the continuity requirements in contingency plans to maintain essential missions and business functions despite the loss of primary telecommunications services. Organizations may specify different time-periods for primary/alternate sites. Alternate telecommunications services include, for example, additional organizational or commercial ground-based circuits/lines or satellites in lieu of ground-based communications. Organizations consider factors such as availability, quality of service, and access when entering alternate telecommunications agreements.

PRIORITY OF SERVICE PROVISIONS

name: CP-8 (1)

statement

item
name: CP-8 (1)(a)

Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives); and

item
name: CP-8 (1)(b)

Request Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness if the primary and/or alternate telecommunications services are provided by a common carrier.

guidance

Organizations consider the potential mission/business impact in situations where telecommunications service providers are servicing other organizations with similar priority-of-service provisions.
None

SINGLE POINTS OF FAILURE

name: CP-8 (2)

statement

Obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

guidance

None.
None

SEPARATION OF PRIMARY AND ALTERNATE PROVIDERS

name: CP-8 (3)

statement

Obtain alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.

guidance

Threats that affect telecommunications services are typically defined in organizational assessments of risk and include, for example, natural disasters, structural failures, hostile cyber/ physical attacks, and errors of omission/commission. Organizations seek to reduce common susceptibilities by, for example, minimizing shared infrastructure among telecommunications service providers and achieving sufficient geographic separation between services. Organizations may consider using a single service provider in situations where the service provider can provide alternate telecommunications services meeting the separation needs addressed in the risk assessment.
None

PROVIDER CONTINGENCY PLAN

organization-defined frequency
organization-defined frequency

name: CP-8 (4)

statement

item

name: CP-8 (4)(a)

Require primary and alternate telecommunications service providers to have contingency plans;

item

name: CP-8 (4)(b)

Review provider contingency plans to ensure that the plans meet organizational contingency requirements; and

item
name: CP-8 (4)(c)

Obtain evidence of contingency testing and training by providers .

guidance

Reviews of provider contingency plans consider the proprietary nature of such plans. In some situations, a summary of provider contingency plans may be sufficient evidence for organizations to satisfy the review requirement. Telecommunications service providers may also participate in ongoing disaster recovery exercises in coordination with the Department of Homeland Security, state, and local governments. Organizations may use these types of activities to satisfy evidentiary requirements related to service provider contingency plan reviews, testing, and training.

ALTERNATE TELECOMMUNICATION SERVICE TESTING

organization-defined frequency
organization-defined frequency
name: CP-8 (5)

statement

Test alternate telecommunication services .

guidance

CP-3.
None

References
NIST Special Publication 800-34

SYSTEM BACKUP

organization-defined frequency consistent with recovery time and recovery point objectives
organization-defined frequency consistent with recovery time and recovery point objectives

organization-defined frequency consistent with recovery time and recovery point objectives
organization-defined frequency consistent with recovery time and recovery point objectives

organization-defined frequency consistent with recovery time and recovery point objectives
organization-defined frequency consistent with recovery time and recovery point objectives

name: CP-9

statement

item
name: CP-9a.

Conduct backups of user-level information contained in the system ;

item
name: CP-9b.

Conduct backups of system-level information contained in the system ;

item
name: CP-9c.

Conduct backups of system documentation including security-related documentation ; and

item
name: CP-9d.

Protect the confidentiality, integrity, and availability of backup information at storage locations.

guidance

System-level information includes, for example, system-state information, operating system software, application software, and licenses. User-level information includes any information other than system-level information. Mechanisms employed to protect the integrity of system backups include, for example, digital signatures and cryptographic hashes. Protection of backup information while in transit is beyond the scope of this control. System backups reflect the requirements in contingency plans as well as other organizational requirements for backing up information.

TESTING FOR RELIABILITY AND INTEGRITY

organization-defined frequency
organization-defined frequency
name: CP-9 (1)

statement

Test backup information to verify media reliability and information integrity.

guidance

None.

TEST RESTORATION USING SAMPLING

name: CP-9 (2)

statement

Use a sample of backup information in the restoration of selected system functions as part of contingency plan testing.

guidance

SEPARATE STORAGE FOR CRITICAL INFORMATION

organization-defined critical system software and other security-related information
organization-defined critical system software and other security-related information
name: CP-9 (3)

statement

Store backup copies of in a separate facility or in a fire-rated container that is not collocated with the operational system.

guidance

Critical system software includes, for example, operating systems, cryptographic key management systems, and intrusion detection/prevention systems. Security-related information includes, for example, organizational inventories of hardware, software, and firmware components. Alternate storage sites typically serve as separate storage facilities for organizations.

PROTECTION FROM UNAUTHORIZED MODIFICATION

name: CP-9 (4)

statement

Incorporated into CP-9.

TRANSFER TO ALTERNATE STORAGE SITE

organization-defined time-period and transfer rate consistent with the recovery time and recovery point objectives
organization-defined time-period and transfer rate consistent with the recovery time and recovery point objectives
name: CP-9 (5)

statement

Transfer system backup information to the alternate storage site .

guidance

System backup information can be transferred to alternate storage sites either electronically or by physical shipment of storage media.

REDUNDANT SECONDARY SYSTEM

name: CP-9 (6)

statement

Conduct system backup by maintaining a redundant secondary system that is not collocated with the primary system and that can be activated without loss of information or disruption to operations.

guidance

DUAL AUTHORIZATION

organization-defined backup information
organization-defined backup information
name: CP-9 (7)

statement

Enforce dual authorization for the deletion or destruction of .

guidance

Dual authorization ensures that the deletion or destruction of backup information cannot occur unless two qualified individuals carry out the task. Individuals deleting/destroying backup information possess sufficient skills/expertise to determine if the proposed deletion/destruction of backup information reflects organizational policies and procedures. Dual authorization may also be known as two-person control.

CRYPTOGRAPHIC PROTECTION

organization-defined backup information
organization-defined backup information
name: CP-9 (8)

statement

Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of .

guidance

The selection of cryptographic mechanisms is based on the need to protect the confidentiality and integrity of backup information. The strength of mechanism is commensurate with the security category and/or classification of the information. This control enhancement applies to system backup information in storage at primary and alternate locations. Organizations implementing cryptographic mechanisms to protect information at rest also consider cryptographic key management solutions.

References
FIPS Publication 140-2
NIST Special Publication 800-34

SYSTEM RECOVERY AND RECONSTITUTION

organization-defined time-period consistent with recovery time and recovery point objectives
organization-defined time-period consistent with recovery time and recovery point objectives
name: CP-10

statement

Provide for the recovery and reconstitution of the system to a known state after a disruption, compromise, or failure within .

guidance

Recovery is executing contingency plan activities to restore organizational missions and business functions. Reconstitution takes place following recovery and includes activities for returning systems to fully operational states. Recovery and reconstitution operations reflect mission and business priorities, recovery point, time, and reconstitution objectives, and established organizational metrics consistent with contingency plan requirements. Reconstitution includes the deactivation of any interim system capabilities that may have been needed during recovery operations. Reconstitution also includes assessments of fully restored system capabilities, reestablishment of continuous monitoring activities, system reauthorizations (if required), and activities to prepare the systems against future disruptions, compromises, or failures. Recovery and reconstitution capabilities employed by organizations can include both automated mechanisms and manual procedures.

CONTINGENCY PLAN TESTING

name: CP-10 (1)

statement

Incorporated into CP-4.

TRANSACTION RECOVERY

name: CP-10 (2)

statement

Implement transaction recovery for systems that are transaction-based.

guidance

Transaction-based systems include, for example, database management systems and transaction processing systems. Mechanisms supporting transaction recovery include, for example, transaction rollback and transaction journaling.
None

COMPENSATING SECURITY CONTROLS

name: CP-10 (3)
Chapter 3

statement

Addressed through tailoring procedures.

RESTORE WITHIN TIME-PERIOD

organization-defined restoration time-periods
organization-defined restoration time-periods
name: CP-10 (4)

statement

Provide the capability to restore system components within from configuration-controlled and integrity-protected information representing a known, operational state for the components.

guidance

Restoration of system components includes, for example, reimaging which restores components to known, operational states.

FAILOVER CAPABILITY

name: CP-10 (5)

statement

Incorporated into SI-13.

COMPONENT PROTECTION

name: CP-10 (6)

statement

Protect system components used for backup and restoration.

guidance

Protection of system backup and restoration components (hardware, firmware, and software) includes both physical and technical safeguards. Backup and restoration software includes, for example, router tables, compilers, and other security-relevant system software.

References

NIST Special Publication 800-34

ALTERNATE COMMUNICATIONS PROTOCOLS

organization-defined alternative communications protocols
organization-defined alternative communications protocols
name: CP-11

statement

Provide the capability to employ in support of maintaining continuity of operations.

guidance

Contingency plans and the training/testing associated with those plans, incorporate an alternate communications protocol capability as part of establishing resilience in organizational systems. Alternate communications protocols include, for example, switching from TCP/IP Version 4 to TCP/IP Version 6. Switching communications protocols may affect software applications and operational aspects of systems. Organizations assess the potential side effects of introducing such alternate communications protocols prior to implementation.

SAFE MODE

organization-defined conditions
organization-defined conditions

organization-defined restrictions of safe mode of operation
organization-defined restrictions of safe mode of operation
name: CP-12

statement

When are detected, enter a safe mode of operation with .

guidance

For systems supporting critical missions and business functions including, for example, military operations and weapons systems, civilian space operations, nuclear power plant operations, and air traffic control operations (especially real-time operational environments), organizations can identify certain conditions under which those systems revert to a predefined safe mode of operation. The safe mode of operation, which can be activated automatically or manually, restricts the activities or operations systems can execute when those conditions are encountered. Restriction includes, for example, allowing only certain functions that can be carried out under limited power or with reduced communications bandwidth.

ALTERNATIVE SECURITY MECHANISMS

organization-defined alternative or supplemental security mechanisms
organization-defined alternative or supplemental security mechanisms

organization-defined security functions
organization-defined security functions
name: CP-13

statement

Employ for satisfying when the primary means of implementing the security function is unavailable or compromised.

guidance

This control supports system resiliency, contingency planning, and continuity of operations. To ensure mission and business continuity, organizations can implement alternative or supplemental security mechanisms. These mechanisms may be less effective than the primary mechanisms. However, having the capability to readily employ these alternative or supplemental mechanisms, enhances mission and business continuity that might otherwise be adversely impacted if operations had to be curtailed until the primary means of implementing the functions was restored. Given the cost and level of effort required to provide such alternative capabilities, this control is typically applied only to critical security capabilities provided by systems, system components, or system services. For example, an organization may issue to senior executives and system administrators one-time pads if multifactor tokens, the standard means for secure remote authentication, is compromised.
CP-2 CP-11

IDENTIFICATION AND AUTHENTICATION

IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES

organization-defined personnel or roles
organization-defined personnel or roles

organization-defined senior management official
organization-defined senior management official

organization-defined frequency
organization-defined frequency

organization-defined frequency
organization-defined frequency

name: IA-1

statement

item
name: IA-1a.

Develop, document, and disseminate to :

item
name: IA-1a.1.

An identification and authentication policy that:

item
name: IA-1a.1.(a)

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

item
name: IA-1a.1.(b)

Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and

item
name: IA-1a.2.

Procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls;

item
name: IA-1b.

Designate an to manage the identification and authentication policy and procedures;

item
name: IA-1c.

Review and update the current identification and authentication:

item
name: IA-1c.1.

Policy ; and

item
name: IA-1c.2.

Procedures ;

item
name: IA-1d.

Ensure that the identification and authentication procedures implement the identification and authentication policy and controls; and

item
name: IA-1e.

Develop, document, and implement remediation actions for violations of the identification and authentication policy.

guidance

This control addresses the establishment of policy and procedures for the effective implementation of the controls and control enhancements in the IA family. The risk management strategy is an important factor in establishing policy and procedures. Comprehensive policy and procedures help provide security and privacy assurance. Security and privacy program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general security and privacy policy or can be represented by multiple policies reflecting the complex nature of organizations. The procedures can be established for security and privacy programs and for systems, if needed. Procedures describe how policies or controls are implemented and can be directed at the personnel or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. It is important to recognize that restating controls does not constitute an organizational policy or procedure.

References

FIPS Publication 201
NIST Special Publication 800-12
NIST Special Publication 800-30
NIST Special Publication 800-39
NIST Special Publication 800-63
NIST Special Publication 800-73
NIST Special Publication 800-76
NIST Special Publication 800-78
NIST Special Publication 800-100

IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

name: IA-2

statement

Uniquely identify and authenticate organizational users or processes acting on behalf of organizational users.

guidance

Organizations can satisfy the identification and authentication requirements in this control by complying with the requirements in Homeland Security Presidential Directive 12. Organizational users include employees or individuals that organizations consider having the equivalent status of employees including, for example, contractors and guest researchers. This control applies to all accesses other than accesses that are explicitly identified in AC-14 and that occur through the authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts or for detailed accountability of individual activity. Organizations employ passwords, physical authenticators, or biometrics to authenticate user identities, or in the case of multifactor authentication, some combination thereof. Access to organizational systems is defined as either local access or network access. Local access is any access to organizational systems by users or processes acting on behalf of users, where such access is obtained through direct connections without the use of networks. Network access is access to organizational systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks. Internal networks include local area networks and wide area networks. The use of encrypted virtual private networks for network connections between organization-controlled endpoints and non-organization controlled endpoints may be treated as internal networks with respect to protecting the confidentiality and integrity of information traversing the network. Identification and authentication requirements for non-organizational users are described in IA-8.

MULTIFACTOR AUTHENTICATION TO PRIVILEGED ACCOUNTS

name: IA-2 (1)

statement

Implement multifactor authentication for access to privileged accounts.

guidance

Multifactor authentication requires the use of two or more different factors to achieve authentication. Factors are defined as follows: something you know, for example, a password or personal identification number (PIN); something you have, for example, a physical authenticator or cryptographic identification device; or something you are, for example, a biometric. Multifactor solutions that feature physical authenticators include, for example, hardware authenticators providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card or the DoD common access card. In addition to authenticating users at the system level (i.e., at logon), organizations may also employ authentication mechanisms at the application level, at their discretion, to provide increased information security. Regardless of the type of access (i.e., local, network, or remote) privileged accounts are always authenticated using multifactor options appropriate for the level

of risk. Organizations can add additional security measures, such as additional or more rigorous authentication mechanisms, for specific types of access.

MULTIFACTOR AUTHENTICATION TO NON-PRIVILEGED ACCOUNTS

name: IA-2 (2)

statement

Implement multifactor authentication for access to non-privileged accounts.

guidance

Multifactor authentication requires the use of two or more different factors to achieve authentication. Factors are defined as follows: something you know, for example, a personal identification number (PIN); something you have, for example, a physical authenticator or cryptographic private key stored in hardware or software; or something you are, for example, a biometric. Multifactor solutions that feature physical authenticators include, for example, hardware authenticators providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card or the DoD common access card. In addition to authenticating users at the system level, organizations may also employ authentication mechanisms at the application level, at their discretion, to provide increased information security. Organizations can also provide additional security measures, such as additional or more rigorous authentication mechanisms, for specific types of access.

LOCAL ACCESS TO PRIVILEGED ACCOUNTS

name: IA-2 (3)
IA-2(1)(2)

statement

Incorporated into IA-2(1)(2).

LOCAL ACCESS TO NON-PRIVILEGED ACCOUNTS

name: IA-2 (4)
IA-2(1)(2)

statement

Incorporated into IA-2(1)(2).

INDIVIDUAL AUTHENTICATION WITH GROUP AUTHENTICATION

name: IA-2 (5)

statement

When shared accounts or authenticators are employed, require users to be individually authenticated before granting access to the shared accounts or resources.

guidance

Individual authentication prior to the shared group authentication helps organizations to mitigate the risk of using group accounts or authenticators.
None

NETWORK ACCESS TO PRIVILEGED ACCOUNTS # SEPARATE DEVICE

name: IA-2 (6)
IA-2(1)(2)

statement

Incorporated into IA-2(1)(2).

NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS # SEPARATE DEVICE

name: IA-2 (7)
IA-2(1)(2)

statement

Incorporated into IA-2(1)(2).

ACCESS TO ACCOUNTS - REPLAY RESISTANT

name: IA-2 (8)

statement

Implement replay-resistant authentication mechanisms for access to [Selection (one or more): privileged accounts; non-privileged accounts].

guidance

Authentication processes resist replay attacks if it is impractical to achieve successful authentications by replaying previous authentication messages. Replay-resistant techniques include, for example, protocols that use nonces or challenges such as time synchronous or challenge-response one-time authenticators.
None

NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS # REPLAY RESISTANT

name: IA-2 (9)
IA-2(8)

statement

Incorporated into IA-2(8).

SINGLE SIGN-ON

organization-defined system accounts and services
organization-defined system accounts and services
name: IA-2 (10)

statement

Provide a single sign-on capability for .

guidance

Single sign-on enables users to log in once and gain access to multiple system resources. Organizations consider the operational efficiencies provided by single sign-on capabilities with the risk introduced by allowing access to multiple systems via a single authentication event. Single sign-on can present opportunities to improve system security, for example by providing the ability to add multifactor authentication for applications that may not be able to natively support this function. This situation may occur in legacy applications or systems.
None

REMOTE ACCESS # SEPARATE DEVICE

name: IA-2 (11)
IA-2(1)(2)

statement

Incorporated into IA-2(1)(2).

ACCEPTANCE OF PIV CREDENTIALS

name: IA-2 (12)

statement

Accept and electronically verify Personal Identity Verification credentials.

guidance

This control enhancement applies to organizations implementing logical access control and physical access control systems. Personal Identity Verification (PIV) credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents. The adequacy and reliability of PIV card issuers are addressed and authorized using NIST Special Publication 800-79. Acceptance of PIV credentials includes derived PIV credentials, the use of which is addressed in NIST Special Publication 800-166.
None

OUT-OF-BAND AUTHENTICATION

name: IA-2 (13)
IA-2(1)(2)

statement

Incorporated into IA-2(1)(2).

References

FIPS Publication 140-2
FIPS Publication 201
NIST Special Publication 800-63
NIST Special Publication 800-73
NIST Special Publication 800-76
NIST Special Publication 800-78

DEVICE IDENTIFICATION AND AUTHENTICATION

organization-defined specific and/or types of devices
organization-defined specific and/or types of devices
name: IA-3

statement

Uniquely identify and authenticate before establishing a [Selection (one or more): local; remote; network] connection.

guidance

Devices requiring unique device-to-device identification and authentication are defined by type, by device, or by a combination of type and device. Organization-defined device types may include devices that are not owned by the organization. Systems use shared known information (e.g., Media Access Control [MAC] or Transmission Control Protocol/Internet Protocol [TCP/IP] addresses) for device identification or organizational authentication solutions (e.g., IEEE 802.1x and Extensible Authentication Protocol [EAP], RADIUS server with EAP-Transport Layer Security [TLS] authentication, Kerberos) to identify and authenticate devices on local and wide area networks. Organizations determine the required strength of authentication mechanisms based on the security categories of systems and mission/business requirements. Because of the challenges of implementing this control on large scale, organizations can restrict the application of the control to a limited number (and type) of devices based on organizational need.

CRYPTOGRAPHIC BIDIRECTIONAL AUTHENTICATION

organization-defined specific devices and/or types of devices
organization-defined specific devices and/or types of devices
name: IA-3 (1)

statement

Authenticate before establishing [Selection (one or more): local; remote; network] connection using bidirectional authentication that is cryptographically based.

guidance

A local connection is any connection with a device communicating without the use of a network. A network connection is any connection with a device that communicates through a network. A remote connection is any connection with a device communicating through an external network. Bidirectional authentication provides stronger safeguards to validate the identity of other devices for connections that are of greater risk.

CRYPTOGRAPHIC BIDIRECTIONAL NETWORK AUTHENTICATION

name: IA-3 (2)
IA-3(1)

statement

Incorporated into IA-3(1).

DYNAMIC ADDRESS ALLOCATION

organization-defined lease information and lease duration
organization-defined lease information and lease duration
name: IA-3 (3)

statement

item
name: IA-3 (3)(a)

Where addresses are allocated dynamically, standardize dynamic address allocation lease information and the lease duration assigned to devices in accordance with ; and

item
name: IA-3 (3)(b)

Audit lease information when assigned to a device.

guidance

DHCP and DHCPv6 are typical protocols that enable clients to dynamically obtain Internet Protocol address leases from DHCP servers.
None

DEVICE ATTESTATION

organization-defined configuration management process

organization-defined configuration management process
name: IA-3 (4)

statement

Handle device identification and authentication based on attestation by .

guidance

Device attestation refers to the identification and authentication of a device based on its configuration and known operating state. This might be determined via some cryptographic hash of the device. If device attestation is the means of identification and authentication, then it is important that patches and updates to the device are handled via a configuration management process such that the patches and updates are done securely and at the same time do not disrupt the identification and authentication to other devices.

IDENTIFIER MANAGEMENT

organization-defined personnel or roles
organization-defined personnel or roles

organization-defined time-period
organization-defined time-period
name: IA-4

statement

Manage system identifiers by:

item
name: IA-4a.

Receiving authorization from to assign an individual, group, role, or device identifier;

item
name: IA-4b.

Selecting an identifier that identifies an individual, group, role, or device;

item
name: IA-4c.

Assigning the identifier to the intended individual, group, role, or device; and

item
name: IA-4d.

Preventing reuse of identifiers for .

guidance

Common device identifiers include, for example, media access control (MAC), Internet Protocol addresses, or device-unique token identifiers. Management of individual identifiers is not applicable to shared system accounts. Typically, individual identifiers are the user names of the system accounts assigned to those individuals. In such instances, the account management activities of AC-2 use account names provided by IA-4. This control also addresses individual identifiers not necessarily associated with system accounts. Preventing the reuse of identifiers implies preventing the assignment of previously used individual, group, role, or device identifiers to different individuals, groups, roles, or devices.

PROHIBIT ACCOUNT IDENTIFIERS AS PUBLIC IDENTIFIERS

name: IA-4 (1)

statement

Prohibit the use of system account identifiers that are the same as public identifiers for individual electronic mail accounts.

guidance

Prohibiting the use of systems account identifiers that are the same as some public identifier such as the individual identifier section of an electronic mail address, makes it more difficult for adversaries to guess user identifiers on organizational systems. The use of this control alone only complicates guessing of identifiers and must be combined with appropriate protections for authenticators and attributes to protect the account as a whole.

SUPERVISOR AUTHORIZATION

name: IA-4 (2)
IA-12(1)

statement

Incorporated into IA-12(1).

MULTIPLE FORMS OF CERTIFICATION

name: IA-4 (3)
IA-12(2)

statement

Incorporated into IA-12(2).

IDENTIFY USER STATUS

organization-defined characteristic identifying individual status
organization-defined characteristic identifying individual status
name: IA-4 (4)

statement

Manage individual identifiers by uniquely identifying each individual as .

guidance

Characteristics identifying the status of individuals include, for example, contractors and foreign nationals. Identifying the status of individuals by specific characteristics provides additional information about the people with whom organizational personnel are communicating. For example, it might be useful for a government employee to know that one of the individuals on an email message is a contractor.
None

DYNAMIC MANAGEMENT

name: IA-4 (5)

statement

Manage individual identifiers dynamically.

guidance

In contrast to conventional approaches to identification which presume static accounts for preregistered users, many distributed systems establish identifiers at run time for entities that were previously unknown. In these situations, organizations anticipate and provision for the dynamic establishment of identifiers. Pre-established trust relationships and mechanisms with appropriate authorities to validate identities and related credentials are essential.

CROSS-ORGANIZATION MANAGEMENT

organization-defined external organizations
organization-defined external organizations

name: IA-4 (6)

statement

Coordinate with for cross-organization management of identifiers.

guidance

Cross-organization identifier management provides the capability for organizations to appropriately identify individuals, groups, roles, or devices when conducting cross-organization activities involving the processing, storage, or transmission of information.

IN-PERSON REGISTRATION

name: IA-4 (7)
IA-12(4)

statement

Incorporated into IA-12(4).

PAIRWISE PSEUDONYMOUS IDENTIFIERS

name: IA-4 (8)

statement

Generate pairwise pseudonymous identifiers.

guidance

Generating distinct pairwise pseudonymous identifiers, with no identifying information about a subscriber, discourages subscriber activity tracking and profiling beyond the operational requirements established by an organization. The pairwise pseudonymous identifiers are unique to each relying party, except in situations where relying parties show a demonstrable relationship justifying an operational need for correlation, or all parties consent to being correlated in such a manner.

References

FIPS Publication 201
NIST Special Publication 800-63
NIST Special Publication 800-73
NIST Special Publication 800-76
NIST Special Publication 800-78

AUTHENTICATOR MANAGEMENT

organization-defined time-period by authenticator type
organization-defined time-period by authenticator type

name: IA-5

statement

Manage system authenticators by:

item

name: IA-5a.

Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;

item

name: IA-5b.

Establishing initial authenticator content for any authenticators issued by the organization;

item

name: IA-5c.

Ensuring that authenticators have sufficient strength of mechanism for their intended use;

item
name: IA-5d.

Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;

item
name: IA-5e.

Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;

item
name: IA-5f.

Changing/refreshing authenticators ;

item
name: IA-5g.

Protecting authenticator content from unauthorized disclosure and modification;

item
name: IA-5h.

Requiring individuals to take, and having devices implement, specific security controls to protect authenticators; and

item
name: IA-5i.

Changing authenticators for group/role accounts when membership to those accounts changes.

guidance

Examples of individual authenticators include passwords, cryptographic devices, one-time password devices, and key cards. The initial authenticator content is the actual content of the authenticator, for example, the initial password. In contrast, the requirements about authenticator content include, for example, the minimum password length. Developers may ship system components with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant security risk. The requirement to protect individual authenticators may be implemented via control PL-4 or PS-6 for authenticators in the possession of individuals and by controls AC-3, AC-6, and SC-28 for authenticators stored in organizational systems including, for example, passwords stored in hashed or encrypted formats or files containing

encrypted or hashed passwords accessible with administrator privileges. Systems support authenticator management by organization-defined settings and restrictions for various authenticator characteristics including, for example, minimum password length, validation time window for time synchronous one-time tokens, and number of allowed rejections during the verification stage of biometric authentication. Actions that can be taken to safeguard individual authenticators include, for example, maintaining possession of authenticators, not loaning or sharing authenticators with others, and reporting lost, stolen, or compromised authenticators immediately. Authenticator management includes issuing and revoking, when no longer needed, authenticators for temporary access such as that required for remote maintenance. Device authenticators include, for example, certificates and passwords.

PASSWORD-BASED AUTHENTICATION

organization-defined frequency
organization-defined frequency
name: IA-5 (1)

statement

For password-based authentication:

item
name: IA-5 (1)(a)

Maintain a list of commonly-used, expected, or compromised passwords and update the list and when organizational passwords are suspected to have been compromised directly or indirectly;

item
name: IA-5 (1)(b)

Verify, when users create or update passwords, that the passwords are not found on the organization-defined list of commonly-used, expected, or compromised passwords;

item
name: IA-5 (1)(c)

Transmit only cryptographically-protected passwords;

item
name: IA-5 (1)(d)

Store passwords using an approved hash algorithm and salt, preferably using a keyed hash;

item
name: IA-5 (1)(e)

Require immediate selection of a new password upon account recovery;

item

name: IA-5 (1)(f)

Allow user selection of long passwords and passphrases, including spaces and all printable characters; and

item
name: IA-5 (1)(g)

Employ automated tools to assist the user in selecting strong password authenticators.

guidance

This control enhancement applies to passwords regardless of whether they are used in single-factor or multi-factor authentication. Long passwords or passphrases are preferable over shorter passwords. Enforced composition rules provide marginal security benefit while decreasing usability. Account recovery can occur, for example, in situations when a password is forgotten. Cryptographically-protected passwords include, for example, salted one-way cryptographic hashes of passwords. The list of commonly-used, expected, or compromised passwords may include, for example, passwords obtained from previous breach corpuses, dictionary words, and repetitive or sequential characters. Examples include aaaaaaa, 1234abcd, and qwertyuiop. The list can also include context specific words, for example, the name of the service, username, and derivatives thereof.

PUBLIC KEY-BASED AUTHENTICATION

name: IA-5 (2)

statement

For public key-based authentication:

item
name: IA-5 (2)(a)

Enforce authorized access to the corresponding private key; and

item
name: IA-5 (2)(b)

Map the authenticated identity to the account of the individual or group; and

guidance

Public key cryptography is a valid authentication mechanism for individuals and machines/ devices. When PKI is leveraged, status information for certification paths includes, for example, certificate revocation lists or certificate status protocol responses. For PIV cards, the validation of certificates involves the construction and verification of a certification path to the Common Policy Root trust anchor which includes certificate policy processing. Implementing a local cache of revocation data to support path discovery and validation supports system availability in situations where organizations are unable to access revocation information via the network

IN-PERSON OR TRUSTED EXTERNAL PARTY REGISTRATION

name: IA-5 (3)
IA-12(4)

statement

Incorporated into IA-12(4).

AUTOMATED SUPPORT FOR PASSWORD STRENGTH DETERMINATION

name: IA-5 (4)
IA-5(1)

statement

Incorporated into IA-5(1).

CHANGE AUTHENTICATORS PRIOR TO DELIVERY

name: IA-5 (5)

statement

Require developers and installers of system components to provide unique authenticators or change default authenticators prior to delivery and installation.

guidance

This control enhancement extends the requirement for organizations to change default authenticators upon system installation, by requiring developers and/or installers to provide unique authenticators or change default authenticators for system components prior to delivery and/or installation. However, it typically does not apply to the developers of commercial off-the-shelf information technology products. Requirements for unique authenticators can be included in acquisition documents prepared by organizations when procuring systems or system components.
None

PROTECTION OF AUTHENTICATORS

name: IA-5 (6)

statement

Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access.

guidance

For systems containing multiple security categories of information without reliable physical or logical separation between categories, authenticators used to grant access to the systems are protected commensurate with the highest security category of information on the systems. Security categories of information are determined as part of the security categorization process.

NO EMBEDDED UNENCRYPTED STATIC AUTHENTICATORS

name: IA-5 (7)

statement

Ensure that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.

guidance

Organizations exercise caution in determining whether embedded or stored authenticators are in encrypted or unencrypted form. If authenticators are used in the manner stored, then those representations are considered unencrypted authenticators. This is irrespective of whether that representation is perhaps an encrypted version of something else.
None

MULTIPLE SYSTEM ACCOUNTS

organization-defined security safeguards
organization-defined security safeguards
name: IA-5 (8)

statement

Implement to manage the risk of compromise due to individuals having accounts on multiple systems.

guidance

When individuals have accounts on multiple systems, there is the risk that a compromise of one account may lead to the compromise of other accounts if individuals use the same authenticators. Possible alternatives include: having different authenticators on all systems; employing some form of single sign-on mechanism; or using some form of one-time passwords on all systems.
None

FEDERATED CREDENTIAL MANAGEMENT

organization-defined external organizations
organization-defined external organizations
name: IA-5 (9)

statement

Use to federate authenticators.

guidance

Federation provides the capability for organizations to appropriately authenticate individuals and devices when conducting cross-organization activities involving the processing, storage, or transmission of information.

DYNAMIC CREDENTIAL BINDING

name: IA-5 (10)

statement

Bind identities and authenticators dynamically.

guidance

Authentication requires some form of binding between an identity and the authenticator used to confirm the identity. In conventional approaches, this binding is established by pre-provisioning both the identity and the authenticator to the system. For example, the binding between a username (i.e., identity) and a password (i.e., authenticator) is accomplished by provisioning the identity and authenticator as a pair in the system. New authentication techniques allow the binding between the identity and the authenticator to be implemented outside a system. For example, with smartcard credentials, the identity and the authenticator are bound together on the smartcard. Using these credentials, systems can authenticate identities that have not been pre-provisioned, dynamically provisioning the identity after authentication. In these situations, organizations can anticipate the dynamic provisioning of identities. Pre-established trust relationships and mechanisms with appropriate authorities to validate identities and related credentials are essential.

HARDWARE TOKEN-BASED AUTHENTICATION

name: IA-5 (11)
IA-2(1)(2)

statement

Incorporated into IA-2(1)(2).

BIOMETRIC AUTHENTICATION PERFORMANCE

organization-defined biometric quality requirements
organization-defined biometric quality requirements
name: IA-5 (12)

statement

For biometric-based authentication, employ mechanisms that satisfy .

guidance

Unlike password-based authentication which provides exact matches of user-input passwords to stored passwords, biometric authentication does not provide such exact matches. Depending upon the type of biometric and the type of collection mechanism, there is likely to be some divergence from the presented biometric and stored biometric which serves as the basis of comparison. The matching performance is the rate at which a biometric algorithm correctly results in a match for a genuine user and rejects other users. Biometric performance requirements include, for example, the match rate as this reflects the accuracy of the biometric matching algorithm being used by a system.

EXPIRATION OF CACHED AUTHENTICATORS

organization-defined time-period
organization-defined time-period
name: IA-5 (13)

statement

Prohibit the use of cached authenticators after .

guidance

None.
None

MANAGING CONTENT OF PKI TRUST STORES

name: IA-5 (14)

statement

For PKI-based authentication, employ a deliberate organization-wide methodology for managing the content of PKI trust stores installed across all platforms including networks, operating systems, browsers, and applications.

guidance

None.
None

GSA-APPROVED PRODUCTS AND SERVICES

name: IA-5 (15)

statement

Use only General Services Administration-approved and validated products and services.

guidance

General Services Administration (GSA)-approved products and services are the products and services that have been approved through the GSA conformance program, where applicable, and posted to the GSA Approved Products List.
None

IN-PERSON OR TRUSTED EXTERNAL PARTY AUTHENTICATOR ISSUANCE

organization-defined types of and/or specific authenticators
organization-defined types of and/or specific authenticators

organization-defined registration authority
organization-defined registration authority

organization-defined personnel or roles
organization-defined personnel or roles
name: IA-5 (16)

statement

Require that the issuance of be conducted [Selection: in person; by a trusted external party] before with authorization by .

guidance

None.

PRESENTATION ATTACK DETECTION FOR BIOMETRIC AUTHENTICATORS

name: IA-5 (17)

statement

Employ presentation attack detection mechanisms for biometric-based authentication.

guidance

Biometric characteristics do not constitute secrets. Such characteristics can be obtained by online web accesses; taking a picture of someone with a camera phone to obtain facial images with or without their knowledge; lifting from objects that someone has touched, for example, a latent fingerprint; or capturing a high-resolution image, for example, an iris pattern. Presentation attack detection technologies including, for example, liveness detection, can mitigate the risk of these types of attacks by making it more difficult to produce artifacts intended to defeat the biometric sensor.

References

FIPS Publication 201
NIST Special Publication 800-73
NIST Special Publication 800-63
NIST Special Publication 800-76
NIST Special Publication 800-78

AUTHENTICATOR FEEDBACK

name: IA-6

statement

Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.

guidance

The feedback from systems does not provide information that would allow unauthorized individuals to compromise authentication mechanisms. For some types of systems or system components, for example, desktops/notebooks with relatively large monitors, the threat (referred to as shoulder surfing) may be significant. For other types of systems or components, for example, mobile devices with small displays, this threat may be less significant, and is balanced against the increased likelihood of typographic input errors due to the small keyboards. Therefore, the means for obscuring authenticator feedback is selected accordingly. Obscuring authenticator feedback includes, for example, displaying asterisks when users type passwords into input devices, or displaying feedback for a very limited time before fully obscuring it.

CRYPTOGRAPHIC MODULE AUTHENTICATION

name: IA-7

statement

Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidelines for such authentication.

guidance

Authentication mechanisms may be required within a cryptographic module to authenticate an operator accessing the module and to verify that the operator is authorized to assume the requested role and perform services within that role.

References

FIPS Publication 140-2

IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)

name: IA-8

statement

Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.

guidance

Non-organizational users include system users other than organizational users explicitly covered by IA-2. These individuals are uniquely identified and authenticated for accesses other than those accesses explicitly identified and documented in AC-14. Identification and authentication of non-organizational users accessing federal systems may be required to protect federal, proprietary, or privacy-related information (with exceptions noted for national security systems). Organizations consider many factors including scalability, practicality, security, and privacy in balancing the need to ensure ease of use for access to federal information and systems with the need to protect and adequately mitigate risk.

ACCEPTANCE OF PIV CREDENTIALS FROM OTHER AGENCIES

name: IA-8 (1)

statement

Accept and electronically verify Personal Identity Verification credentials from other federal agencies.

guidance

This control enhancement applies to both logical and physical access control systems. Personal Identity Verification (PIV) credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidelines. The adequacy and reliability of PIV card issuers are addressed and authorized using NIST Special Publication 800-79.

ACCEPTANCE OF EXTERNAL CREDENTIALS

name: IA-8 (2)

statement

Accept only external credentials that are NIST compliant.

guidance

This control enhancement applies to organizational systems that are accessible to the public, for example, public-facing websites. External credentials are those credentials issued by nonfederal

government entities. Such credentials are certified as compliant with NIST Special Publication 800-63 by an approved accreditation authority. Approved external credentials meet or exceed the set of minimum federal government-wide technical, security, privacy, and organizational maturity requirements. This allows federal government relying parties to trust such credentials at their approved assurance levels.
None

USE OF FICAM-APPROVED PRODUCTS

name: IA-8 (3)
IA-8(2)

statement

Incorporated into IA-8(2).

USE OF NIST-ISSUED PROFILES

name: IA-8 (4)

statement

Conform to NIST-issued profiles for identity management.

guidance

This control enhancement addresses open identity management standards. To ensure that these identity management standards are viable, robust, reliable, sustainable, and interoperable as documented, the United States Government assesses and scopes the standards and technology implementations against applicable laws, Executive Orders, directives, policies, regulations, standards, and guidelines. The result is NIST-issued implementation profiles of approved protocols.
None

ACCEPTANCE OF PIV-I CREDENTIALS

name: IA-8 (5)

statement

Accept and electronically verify Personal Identity Verification-I (PIV-I) credentials.

guidance

This control enhancement applies to both logical access control and physical access control systems. It addresses Nonfederal Issuers of identity cards that desire to interoperate with United States Government Personal Identity Verification (PIV) systems and that can be trusted by federal government-relying parties. The X.509 certificate policy for the Federal Bridge Certification Authority (FBCA) addresses PIV-I requirements. The PIV-I card is commensurate with the PIV credentials as defined in cited references. PIV-I credentials are the credentials issued by a PIV-I provider whose PIV-I certificate policy maps to the Federal Bridge PIV-I

Certificate Policy. A PIV-I provider is cross-certified with the FBCA (directly or through another PKI bridge) with policies that have been mapped and approved as meeting the requirements of the PIV-I policies defined in the FBCA certificate policy.
None

DISASSOCIABILITY

organization-defined measures
organization-defined measures
name: IA-8 (6)

statement

Implement to disassociate user attributes or credential assertion relationships among individuals, credential service providers, and relying parties.

guidance

Federated identity solutions can create increased privacy risks due to tracking and profiling of individuals. Using identifier mapping tables or privacy-enhancing cryptographic techniques to blind credential service providers and relying parties from each other or to make identity attributes less visible to transmitting parties can reduce these privacy risks.
None

References

FIPS Publication 201
NIST Special Publication 800-63
NIST Special Publication 800-116

SERVICE IDENTIFICATION AND AUTHENTICATION

organization-defined system services and applications
organization-defined system services and applications
name: IA-9

statement

Identify and authenticate before establishing communications with devices, users, or other services or applications.

guidance

Services that may require identification and authentication include, for example, web applications using digital certificates or services/applications that query a database. Identification and authentication methods for system services/applications include, for example, information or code signing, provenance graphs, and/or electronic signatures indicating the sources of services.

INFORMATION EXCHANGE

name: IA-9 (1)

statement

Ensure that service providers receive, validate, and transmit identification and authentication information.

guidance

None.
None

TRANSMISSION OF DECISIONS

organization-defined services
organization-defined services

name: IA-9 (2)

statement

Transmit identification and authentication decisions between consistent with organizational policies.

guidance

For distributed architectures, the decisions regarding the validation of identification and authentication claims may be made by services separate from the services acting on those decisions. In such situations, it is necessary to provide the identification and authentication decisions (instead of the actual identifiers and authenticators) to the services that need to act on those decisions.

ADAPTIVE AUTHENTICATION

organization-defined supplemental authentication techniques or mechanisms
organization-defined supplemental authentication techniques or mechanisms

organization-defined circumstances or situations
organization-defined circumstances or situations

name: IA-10

statement

Require individuals accessing the system to employ under specific .

guidance

Adversaries may compromise individual authentication mechanisms and subsequently attempt to impersonate legitimate users. This situation can potentially occur with any authentication mechanisms employed by organizations. To address this threat, organizations may employ specific techniques or mechanisms and establish protocols to assess suspicious behavior. Such behavior may include, for example, accessing information that individuals do not typically access as part of their duties, roles, or responsibilities; accessing greater quantities of information than the individuals would routinely access; or attempting to access information from suspicious network addresses. In situations when pre-established conditions or triggers occur, organizations can require individuals to provide additional authentication information. Another potential use for adaptive authentication is to increase the strength of mechanism based on the number and/or types of records being accessed. Adaptive authentication does not replace and is not used to avoid multifactor mechanisms, but can augment implementations of these controls.

References

NIST Special Publication 800-63

RE-AUTHENTICATION

organization-defined circumstances or situations requiring re-authentication
organization-defined circumstances or situations requiring re-authentication
name: IA-11

statement

Require users to re-authenticate when .

guidance

In addition to the re-authentication requirements associated with device locks, organizations may require re-authentication of individuals in certain situations including, for example, when authenticators or roles change; when security categories of systems change; when the execution of privileged functions occurs; after a fixed time-period; or periodically.

IDENTITY PROOFING

name: IA-12

statement

item

name: IA-12a.

Identity proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines;

item
name: IA-12b.

Resolve user identities to a unique individual; and

item
name: IA-12c.

Collect, validate, and verify identity evidence.

guidance

Identity proofing is the process of collecting, validating, and verifying user#s identity information for the purposes of issuing credentials for accessing a system. This control is intended to mitigate threats to the registration of users and the establishment of their accounts. Standards and guidelines specifying identity assurance levels for identity proofing include NIST Special Publications 800-63 and 800-63A.

SUPERVISOR AUTHORIZATION

name: IA-12 (1)

statement

Require that the registration process to receive an account for logical access includes supervisor or sponsor authorization.

guidance

None.
None

IDENTITY EVIDENCE

name: IA-12 (2)

statement

Require evidence of individual identification be presented to the registration authority.

guidance

Requiring identity evidence, such as documentary evidence or a combination of documents and biometrics, reduces the likelihood of individuals using fraudulent identification to establish an identity, or at least increases the work factor of potential adversaries. Acceptable forms of evidence are consistent with the risk to the systems, roles, and privileges associated with the user#s account.
None

IDENTITY EVIDENCE VALIDATION AND VERIFICATION

organizational defined methods of validation and verification

organizational defined methods of validation and verification
name: IA-12 (3)

statement

Require that the presented identity evidence be validated and verified through .

guidance

Validating and verifying identity evidence increases the assurance that that accounts, identifiers, and authenticators are being issued to the correct user. Validation refers to the process of confirming that the evidence is genuine and authentic and that the data contained in the evidence is correct, current, and related to an actual person or individual. Verification confirms and establishes a linkage between the claimed identity and the actual existence of the user presenting the evidence. Acceptable methods for validating and verifying identity evidence are consistent with the risk to the systems, roles, and privileges associated with the users account
None

IN-PERSON VALIDATION AND VERIFICATION

name: IA-12 (4)

statement

Require that the validation and verification of identity evidence be conducted in person before a designated registration authority.

guidance

In-person proofing reduces the likelihood of fraudulent credentials being issued because it requires the physical presence of individuals, the presentation of physical identity documents, and actual face-to-face interactions with designated registration authorities.
None

ADDRESS CONFIRMATION

name: IA-12 (5)

statement

Require that a [Selection: registration code; notice of proofing] be delivered through an out-of-band channel to verify the users address (physical or digital) of record.

guidance

To make it more difficult for adversaries to pose as legitimate users during the identity proofing process, organizations can use out-of-band methods to increase assurance that the individual associated with an address of record was the same person that participated in the registration. Confirmation can take the form of a temporary enrollment code or a notice of proofing. The delivery address for these artifacts are obtained from records and not self-asserted by the user.

The address can include a physical or a digital address. A home address is an example of a physical address. Email addresses and telephone numbers are examples of digital addresses.

ACCEPT EXTERNALLY-PROOFED IDENTITIES

organization-defined identity assurance level
organization-defined identity assurance level
name: IA-12 (6)

statement

Accept externally-proofed identities at .

guidance

To limit unnecessary re-proofing of identities, particularly of non-PIV users, organizations accept proofing conducted at a commensurate level of assurance by other agencies or organizations. Proofing is consistent with organizational security policy and with the identity assurance level appropriate for the system, application, or information accessed. This is a core component of managing federated identities across agencies and organizations.

References

FIPS Publication 201
NIST Special Publication 800-63

INDIVIDUAL PARTICIPATION

INDIVIDUAL PARTICIPATION POLICY AND PROCEDURES

organization-defined personnel or roles
organization-defined personnel or roles

organization-defined senior management official
organization-defined senior management official

organization-defined frequency
organization-defined frequency

organization-defined frequency
organization-defined frequency
name: IP-1

statement

item
name: IP-1a.

Develop, document, and disseminate to :

item
name: IP-1a.1.

An individual participation policy that:

item
name: IP-1a.1.(a)

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

item
name: IP-1a.1.(b)

Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and

item
name: IP-1a.2.

Procedures to facilitate the implementation of the individual participation policy and the associated individual participation controls;

item
name: IP-1b.

Designate an to manage the individual participation policy and procedures;

item
name: IP-1c.

Review and update the current individual participation:

item
name: IP-1c.1.

Policy ; and

item
name: IP-1c.2.

Procedures ;

item
name: IP-1d.

Ensure that the individual participation procedures implement the individual participation policy and controls; and

item
name: IP-1e.

Develop, document, and implement remediation actions for violations of the individual participation policy.

guidance

This control addresses the establishment of policy and procedures for the effective implementation of the controls and control enhancements in the IP family. The risk management strategy is an important factor in establishing policy and procedures. Comprehensive policy and procedures help provide security and privacy assurance. Security and privacy program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general security and privacy policy or can be represented by multiple policies reflecting the complex nature of organizations. The procedures can be established for security and privacy programs and for systems, if needed. Procedures describe how policies or controls are implemented and can be directed at the personnel or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. It is important to recognize that restating controls does not constitute an organizational policy or procedure.

References

NIST Special Publication 800-12
NIST Special Publication 800-30
NIST Special Publication 800-39
NIST Special Publication 800-100

CONSENT

organization-defined tools or mechanisms
organization-defined tools or mechanisms
name: IP-2

statement

Implement for users to authorize the processing of their personally identifiable information prior to its collection that:

item
name: IP-2a.

Use plain language and provide examples to illustrate the potential privacy risks of the authorization; and

item

name: IP-2b.

Provide a means for users to decline the authorization.

guidance

This control transfers risk that arises from the processing of personally identifiable information from the organization to an individual. It is only selected as required by law or regulation or when individuals can be reasonably expected to understand and accept any privacy risks arising from their authorization. Organizations consider whether other controls may more effectively mitigate privacy risk either alone or in conjunction with consent. To help users understand the risks being accepted when providing consent, organizations write materials in plain language and avoid technical jargon. The examples required in IP-2 a. focus on key points necessary for user decision-making. When developing or purchasing consent tools, organizations consider the application of good information design procedures in all user-facing consent materials; use of active voice and conversational style; logical sequencing of main points; consistent use of the same word (rather than synonyms) to avoid confusion; the use of bullets, numbers, and formatting where appropriate to aid readability; and legibility of text, such as font style, size, color, and contrast with surrounding background.

ATTRIBUTE MANAGEMENT

name: IP-2 (1)

statement

Allow data subjects to tailor use permissions to selected attributes.

guidance

Allowing individuals to select how specific data attributes may be further used or disclosed beyond the original use may help reduce privacy risk arising from the most sensitive of the data attributes while maintaining utility of the data.
None

JUST-IN-TIME NOTICE OF CONSENT

organization-defined frequency
organization-defined frequency
name: IP-2 (2)

statement

Present authorizations to process personally identifiable information in conjunction with the data action or .

guidance

If the circumstances under which an individual gave consent have changed or a significant amount of time has passed since an individual gave consent for the processing of his or her personally identifiable information, the data subject#s assumption about how the information is being processed might no longer be accurate or reliable. Just-in-time notice can help maintain individual satisfaction with how the personally identifiable information is being processed.
None

References
NIST Special Publication 800-63

REDRESS

name: IP-3

statement

item
name: IP-3a.

Establish and implement a process for individuals to have inaccurate personally identifiable information maintained by the organization corrected or amended; and

item
name: IP-3b.

Establish and implement a process for disseminating corrections or amendments of personally identifiable information to other authorized users of the personally identifiable information.

guidance

Redress supports the ability of individuals to ensure the accuracy of their personally identifiable information held by organizations. Effective redress processes demonstrate organizational commitment to data quality especially in those business functions where inaccurate data may result in inappropriate decisions or the denial of benefits and services to individuals. Organizations use discretion in determining if records are to be corrected or amended, based on the scope of redress requests, the changes sought, and the impact of the changes. Other authorized users of personally identifiable information include, for example, external information-sharing partners. An effective redress process includes: providing effective notice of the existence of a personally identifiable information collection; providing plain language explanations of the processes and mechanisms for requesting access to records; establishing the criteria for submitting requests for correction or amendment of records; implementing resources to analyze and adjudicate requests; implementing means of correcting or amending data collections; and reviewing any decisions that may have been the result of inaccurate information.

NOTICE OF CORRECTION OR AMENDMENT

name: IP-3 (1)

statement

Notify affected individuals if their personally identifiable information has been corrected or amended.

guidance

Where personally identifiable information is corrected or amended, organizations take steps to ensure that all authorized recipients of such information and the individual with which the information is associated, are informed of the corrected or amended information.
None

APPEAL

organization-defined process
organization-defined process
name: IP-3 (2)

statement

Provide for individuals to appeal an adverse decision and have incorrect information amended.

guidance

The Senior Agency Official for Privacy ensures that practical means and mechanisms exist and are accessible for individuals to seek the correction or amendment of their personally identifiable information. Redress processes are clearly defined and publicly available. Additionally, redress processes include the provision of responses to individuals of decisions to deny requests for correction or amendment. The responses include the reasons for the decisions, a means to record individual objections to the decisions, and finally, a means of requesting reviews of the initial determinations.
None

PRIVACY NOTICE

organization-defined frequency
organization-defined frequency
name: IP-4

statement

item

name: IP-4a.

Make privacy notice(s) available to individuals upon first interacting with an organization, and subsequently .

item
name: IP-4b.

Ensure that privacy notices are clear and easy-to-understand, expressing information about personally identifiable information processing in plain language.

guidance

To help users understand how their information is being processed, organizations write materials in plain language and avoid technical jargon. When developing privacy notices, organizations consider the application of good information design procedures in all user-facing materials; use of active voice and conversational style; logical sequencing of main points; consistent use of the same word (rather than synonyms) to avoid confusion; use of bullets, numbers, and formatting where appropriate to aid readability; and legibility of text, such as font style, size, color, and contrast with surrounding background.

JUST-IN-TIME NOTICE OF PRIVACY AUTHORIZATION

organization-defined frequency
organization-defined frequency
name: IP-4 (1)

statement

Present authorizations to process personally identifiable information in conjunction with the data action, or .

guidance

If the circumstances under which an individual gave consent have changed or a significant amount of time has passed since an individual gave consent for the processing of his or her personally identifiable information, the data subject#s assumption about how the information is being processed might no longer be accurate or reliable. Just-in-time notice can help maintain individual satisfaction with or ability to participate in how the personally identifiable information is being processed.

PRIVACY ACT STATEMENTS
name: IP-5

statement

item
name: IP-5a.

Include Privacy Act Statements on organizational forms that collect personally identifiable information, or on separate forms that can be retained by individuals; or

item
name: IP-5b.

Read a Privacy Act Statement to the individual prior to initiating the collection of personally identifiable information verbally.

guidance

Privacy Act Statements provide additional formal notice to individuals from whom the information is being collected, notice of the authority of organizations to collect personally identifiable information; whether providing personally identifiable information is mandatory or optional; the principal purpose or purposes for which the personally identifiable information is to be used; the intended disclosures or routine uses of the information; and the consequences of not providing all or some portion of the information requested. Personally identifiable information may be collected verbally, for example, when conducting telephone interviews or surveys.

INDIVIDUAL ACCESS
name: IP-6

statement

Provide individuals the ability to access their personally identifiable information maintained in organizational systems of records.

guidance

Access affords individuals the ability to review personally identifiable information about them held within organizational systems of records. Access includes timely, simplified, and inexpensive access to data. Organizational processes for allowing access to records may differ based on resources, legal requirements, or other factors. The Senior Agency Official for Privacy is responsible for the content of Privacy Act regulations and record request processing, in consultation with legal counsel. Access to certain types of records may not be appropriate, and heads of agencies may promulgate rules exempting specific systems from the access provision of the Privacy Act. When feasible, those rules will be publicly available. In addition, individuals are not entitled to access to information compiled in reasonable anticipation of a civil action or proceeding.

INCIDENT RESPONSE

INCIDENT RESPONSE POLICY AND PROCEDURES

organization-defined personnel or roles

organization-defined personnel or roles

organization-defined senior management official
organization-defined senior management official

organization-defined frequency
organization-defined frequency

organization-defined frequency
organization-defined frequency
name: IR-1

statement

item
name: IR-1a.

Develop, document, and disseminate to :

item
name: IR-1a.1.

An incident response policy that:

item
name: IR-1a.1.(a)

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

item
name: IR-1a.1.(b)

Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and

item
name: IR-1a.2.

Procedures to facilitate the implementation of the incident response policy and the associated incident response controls;

item
name: IR-1b.

Designate an to manage the incident response policy and procedures;

item
name: IR-1c.

Review and update the current incident response:

item
name: IR-1c.1.

Policy ; and

item
name: IR-1c.2.

Procedures ;

item
name: IR-1d.

Ensure that the incident response procedures implement the incident response policy and controls; and

item
name: IR-1e.

Develop, document, and implement remediation actions for violations of the incident response policy.

guidance

This control addresses the establishment of policy and procedures for the effective implementation of the controls and control enhancements in the IR family. The risk management strategy is an important factor in establishing policy and procedures. Comprehensive policy and procedures help provide security and privacy assurance. Security and privacy program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general security and privacy policy or can be represented by multiple policies reflecting the complex nature of organizations. The procedures can be established for security and privacy programs and for systems, if needed. Procedures describe how policies or controls are implemented and can be directed at the personnel or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. It is important to recognize that restating controls does not constitute an organizational policy or procedure.

References

NIST Special Publication 800-12
NIST Special Publication 800-30
NIST Special Publication 800-39
NIST Special Publication 800-61
NIST Special Publication 800-83
NIST Special Publication 800-100

INCIDENT RESPONSE TRAINING

organization-defined time-period
organization-defined time-period

organization-defined frequency
organization-defined frequency
name: IR-2

statement

Provide incident response training to system users consistent with assigned roles and responsibilities:

item
name: IR-2a.

Within of assuming an incident response role or responsibility;

item
name: IR-2b.

When required by system changes; and

item
name: IR-2c.

thereafter.

guidance

Incident response training is linked to assigned roles and responsibilities of organizational personnel to ensure the appropriate content and level of detail is included in such training. For example, users may only need to know who to call or how to recognize an incident; system administrators may require additional training on how to handle and remediate incidents; and finally, incident responders may receive more specific training on forensics, reporting, system recovery, and restoration. Incident response training includes user training in the identification and reporting of suspicious activities, both from external and internal sources.

SIMULATED EVENTS
name: IR-2 (1)

statement

Incorporate simulated events into incident response training to facilitate effective response by personnel in crisis situations.

guidance

None.
None

AUTOMATED TRAINING ENVIRONMENTS

name: IR-2 (2)

statement

Employ automated mechanisms to provide a more thorough and realistic incident response training environment.

guidance

None.
None

References

NIST Special Publication 800-50

INCIDENT RESPONSE TESTING

organization-defined frequency
organization-defined frequency

organization-defined tests
organization-defined tests

name: IR-3

statement

Test the incident response capability for the system using to determine the incident response effectiveness and documents the results.

guidance

Organizations test incident response capabilities to determine the overall effectiveness of the capabilities and to identify potential weaknesses or deficiencies. Incident response testing includes, for example, the use of checklists, walk-through or tabletop exercises, simulations (parallel/full interrupt), and comprehensive exercises. Incident response testing can also include a determination of the effects on organizational operations, organizational assets, and individuals due to incident response. Use of qualitative and quantitative data aids in determining the effectiveness of incident response processes.

AUTOMATED TESTING

name: IR-3 (1)

statement

Employ automated mechanisms to more thoroughly and effectively test the incident response capability.

guidance

Organizations use automated mechanisms to more thoroughly and effectively test incident response capabilities. This can be accomplished, for example, by providing more complete coverage of incident response issues; by selecting more realistic test scenarios and test environments; and by stressing the response capability.
None

COORDINATION WITH RELATED PLANS

name: IR-3 (2)

statement

Coordinate incident response testing with organizational elements responsible for related plans.

guidance

Organizational plans related to incident response testing include, for example, Business Continuity Plans, Contingency Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Occupant Emergency Plans, and Critical Infrastructure Plans.
None

CONTINUOUS IMPROVEMENT

name: IR-3 (3)

statement

Use qualitative and quantitative data from testing to:

item
name: IR-3 (3)(a)

Determine the effectiveness of incident response processes;

item
name: IR-3 (3)(b)

Continuously improve incident response processes incorporating advanced information security practices; and

item
name: IR-3 (3)(c)

Provide incident response measures and metrics that are accurate, consistent, and in a reproducible format.

guidance

To help incident response activities function as intended, organizations may use of metrics and evaluation criteria to assess incident response programs as part of an effort to continually improve response performance. These efforts facilitate improvement in incident response efficacy and lessen the impact of incidents.
None

References
NIST Special Publication 800-84
NIST Special Publication 800-115

INCIDENT HANDLING
name: IR-4

statement

item
name: IR-4a.

Implement an incident handling capability for security and privacy incidents that includes preparation, detection and analysis, containment, eradication, and recovery;

item
name: IR-4b.

Coordinate incident handling activities with contingency planning activities;

item
name: IR-4c.

Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly; and

item
name: IR-4d.

Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.

guidance

Organizations recognize that incident response capability is dependent on the capabilities of organizational systems and the mission/business processes being supported by those systems. Therefore, organizations consider incident response as part of the definition, design, and development of mission/business processes and systems. Incident-related information can be obtained from a variety of sources including, for example, audit monitoring, network monitoring, physical access monitoring, user/administrator reports, and reported supply chain

events. Effective incident handling capability includes coordination among many organizational entities including, for example, mission/business owners, system owners, authorizing officials, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices, and the risk executive (function).

AUTOMATED INCIDENT HANDLING PROCESSES

name: IR-4 (1)

statement

Employ automated mechanisms to support the incident handling process.

guidance

Automated mechanisms supporting incident handling processes include, for example, online incident management systems; and tools that support collection of live response data, full network packet capture, and forensic analysis.

None

DYNAMIC RECONFIGURATION

organization-defined system components
organization-defined system components

name: IR-4 (2)

statement

Include dynamic reconfiguration of as part of the incident response capability.

guidance

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

CONTINUITY OF OPERATIONS

organization-defined classes of incidents
organization-defined classes of incidents

organization-defined actions to take in response to classes of incidents
organization-defined actions to take in response to classes of incidents

name: IR-4 (3)

statement

Identify and to ensure continuation of organizational missions and business functions.

guidance

Classes of incidents include, for example, malfunctions due to design/implementation errors and omissions, targeted malicious attacks, and untargeted malicious attacks. Appropriate incident response actions include, for example, graceful degradation, system shutdown, fall back to manual mode/alternative technology whereby the system operates differently, employing deceptive measures, alternate information flows, or operating in a mode that is reserved solely for when systems are under attack.
None

INFORMATION CORRELATION

name: IR-4 (4)

statement

Correlate incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.

guidance

Sometimes the nature of a threat event, for example, a hostile attack, is such that it can only be observed by bringing together information from different sources including various reports and reporting procedures established by organizations.
None

AUTOMATIC DISABLING OF SYSTEM

organization-defined security violations
organization-defined security violations

name: IR-4 (5)

statement

Implement a configurable capability to automatically disable the system if are detected.

guidance

None.
None

INSIDER THREATS # SPECIFIC CAPABILITIES

name: IR-4 (6)

statement

Implement an incident handling capability for incidents involving insider threats.

guidance

While many organizations address insider threat incidents as an inherent part of their organizational incident response capability, this control enhancement provides additional emphasis on this type of threat and the need for specific incident handling capabilities (as defined within organizations) to provide appropriate and timely responses.
None

INSIDER THREATS # INTRA-ORGANIZATION COORDINATION

organization-defined components or elements of the organization
organization-defined components or elements of the organization
name: IR-4 (7)

statement

Coordinate an incident handling capability for insider threats across .

guidance

Incident handling for insider threat incidents (including preparation, detection and analysis, containment, eradication, and recovery) requires close coordination among a variety of organizational components or elements to be effective. These components or elements include, for example, mission/business owners, system owners, human resources offices, procurement offices, personnel/physical security offices, operations personnel, and risk executive (function). In addition, organizations may require external support from federal, state, and local law enforcement agencies.
None

CORRELATION WITH EXTERNAL ORGANIZATIONS

organization-defined external organizations
organization-defined external organizations

organization-defined incident information
organization-defined incident information
name: IR-4 (8)

statement

Coordinate with to correlate and share to achieve a cross-organization perspective on incident awareness and more effective incident responses.

guidance

The coordination of incident information with external organizations including, for example, mission/business partners, military/coalition partners, customers, and multi-tiered developers, can provide significant benefits. Cross-organizational coordination with respect to incident handling can serve as an important risk management capability. This capability allows organizations to leverage critical information from a variety of sources to effectively respond to information security-related incidents potentially affecting the organization#s operations, assets, and individuals.

DYNAMIC RESPONSE CAPABILITY

organization-defined dynamic response capabilities
organization-defined dynamic response capabilities
name: IR-4 (9)

statement

Employ to effectively respond to security incidents.

guidance

This control enhancement addresses the timely deployment of new or replacement organizational capabilities in response to security and privacy incidents. This includes capabilities implemented at the mission and business process level and at the system level.
None

SUPPLY CHAIN COORDINATION

name: IR-4 (10)

statement

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

guidance

Organizations involved in supply chain activities include, for example, system/product developers, integrators, manufacturers, packagers, assemblers, distributors, vendors, and resellers. Supply chain incidents include, for example, compromises/breaches involving system components, information technology products, development processes or personnel, and distribution processes or warehousing facilities.

References

NIST Special Publication 800-61

INCIDENT MONITORING

name: IR-5

statement

Track and document system security and privacy incidents.

guidance

Documenting system security and privacy incidents includes, for example, maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics; and evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources including, for example, network monitoring; incident reports; incident response teams; user complaints; audit monitoring; physical access monitoring; and user and administrator reports.

AUTOMATED TRACKING, DATA COLLECTION, AND ANALYSIS

name: IR-5 (1)

statement

Employ automated mechanisms to assist in the tracking of security and privacy incidents and in the collection and analysis of incident information.

guidance

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

References

NIST Special Publication 800-61

INCIDENT REPORTING

organization-defined time-period
organization-defined time-period

organization-defined authorities
organization-defined authorities

name: IR-6

statement

item

name: IR-6a.

Require personnel to report suspected security and privacy incidents to the organizational incident response capability within ; and

item
name: IR-6b.

Report security, privacy, and supply chain incident information to .

guidance

The intent of this control is to address both specific incident reporting requirements within an organization and the incident reporting requirements for organizations. Suspected security incidents include, for example, the receipt of suspicious email communications that can potentially contain malicious code. Suspected privacy incidents include, for example a suspected breach of personally identifiable information or the recognition that the processing of personally identifiable information creates potential privacy risk. The types of incidents reported, the content and timeliness of the reports, and the designated reporting authorities reflect applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines.

AUTOMATED REPORTING

name: IR-6 (1)

statement

Employ automated mechanisms to assist in the reporting of security and privacy incidents.

guidance

None.

VULNERABILITIES RELATED TO INCIDENTS

organization-defined personnel or roles
organization-defined personnel or roles
name: IR-6 (2)

statement

Report system vulnerabilities associated with reported security and privacy incidents to .

guidance

None.
None

SUPPLY CHAIN COORDINATION

name: IR-6 (3)

statement

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

guidance

Organizations involved in supply chain activities include, for example, system/product developers, integrators, manufacturers, packagers, assemblers, distributors, vendors, and resellers. Supply chain incidents include, for example, compromises/breaches involving system components, information technology products, development processes or personnel, and distribution processes or warehousing facilities. Organizations determine the appropriate information to share considering the value gained from support by external organizations with the potential for harm due to controlled unclassified information being released to outside organizations of perhaps questionable trustworthiness.

References

NIST Special Publication 800-61

INCIDENT RESPONSE ASSISTANCE

name: IR-7

statement

Provide an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the system for the handling and reporting of security and privacy incidents.

guidance

Incident response support resources provided by organizations include, for example, help desks, assistance groups, and access to forensics services or consumer redress services, when required.

AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION AND SUPPORT

name: IR-7 (1)

statement

Employ automated mechanisms to increase the availability of incident response-related information and support.

guidance

Automated mechanisms can provide a push and/or pull capability for users to obtain incident response assistance. For example, individuals might have access to a website to query the assistance capability, or the assistance capability can proactively send information to users

(general distribution or targeted) as part of increasing understanding of current response capabilities and support.
None

COORDINATION WITH EXTERNAL PROVIDERS

name: IR-7 (2)

statement

item
name: IR-7 (2)(a)

Establish a direct, cooperative relationship between its incident response capability and external providers of system protection capability; and

item
name: IR-7 (2)(b)

Identify organizational incident response team members to the external providers.

guidance

External providers of a system protection capability include, for example, the Computer Network Defense program within the U.S. Department of Defense. External providers help to protect, monitor, analyze, detect, and respond to unauthorized activity within organizational information systems and networks.
None

INCIDENT RESPONSE PLAN

organization-defined personnel or roles
organization-defined personnel or roles

organization-defined frequency
organization-defined frequency

organization-defined entities, personnel, or roles
organization-defined entities, personnel, or roles

organization-defined incident response personnel (identified by name and/or by role) and organizational elements
organization-defined incident response personnel (identified by name and/or by role) and organizational elements

organization-defined incident response personnel (identified by name and/or by role) and organizational elements
organization-defined incident response personnel (identified by name and/or by role) and organizational elements
name: IR-8

statement

item
name: IR-8a.

Develop an incident response plan that:

item
name: IR-8a.1.

Provides the organization with a roadmap for implementing its incident response capability;

item
name: IR-8a.2.

Describes the structure and organization of the incident response capability;

item
name: IR-8a.3.

Provides a high-level approach for how the incident response capability fits into the overall organization;

item
name: IR-8a.4.

Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;

item
name: IR-8a.5.

Defines reportable incidents;

item
name: IR-8a.6.

Provides metrics for measuring the incident response capability within the organization;

item
name: IR-8a.7.

Defines the resources and management support needed to effectively maintain and mature an incident response capability;

item
name: IR-8a.8.

Is reviewed and approved by ; and

item
name: IR-8a.9.

Explicitly designates responsibility for incident response to .

item
name: IR-8b.

Distribute copies of the incident response plan to ;

item
name: IR-8c.

Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing;

item
name: IR-8d.

Communicate incident response plan changes to ; and

item
name: IR-8e.

Protect the incident response plan from unauthorized disclosure and modification.

guidance

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

PERSONALLY IDENTIFIABLE INFORMATION PROCESSES

organization-defined roles
organization-defined roles
name: IR-8 (1)

statement

Include the following additional processes in the Incident Response Plan for incidents involving personally identifiable information:

item
name: IR-8 (1)(a)

A process to determine if notice to oversight organizations is appropriate and to provide that notice, if appropriate;

item
name: IR-8 (1)(b)

An assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals; and

item
name: IR-8 (1)(c)

A process to ensure prompt reporting by organizational users of any privacy incident to .

guidance

Some organizations may be required by law or policy to provide notice to oversight organizations in the event of a privacy-related incident. Organization-defined roles to which privacy incidents may be reported include, for example, the Senior Agency Official for Privacy, Senior Agency Information Security Officer, Authorizing Official, and System Owner.
None

References
NIST Special Publication 800-61

INFORMATION SPILLAGE RESPONSE

organization-defined personnel or roles
organization-defined personnel or roles

organization-defined actions
organization-defined actions
name: IR-9

statement

Respond to information spills by:

item
name: IR-9a.

Identifying the specific information involved in the system contamination;

item
name: IR-9b.

Alerting of the information spill using a method of communication not associated with the spill;

item
name: IR-9c.

Isolating the contaminated system or system component;

item
name: IR-9d.

Eradicating the information from the contaminated system or component;

item
name: IR-9e.

Identifying other systems or system components that may have been subsequently contaminated; and

item
name: IR-9f.

Performing the following additional actions: .

guidance

Information spillage refers to instances where either classified or controlled unclassified information is inadvertently placed on systems that are not authorized to process such information. Such information spills occur when information that is initially thought to be of lower sensitivity is transmitted to a system and then subsequently determined to be of higher sensitivity. At that point, corrective action is required. The nature of the organizational response is generally based upon the degree of sensitivity of the spilled information, the security capabilities of the system, the specific nature of contaminated storage media, and the access authorizations of individuals with authorized access to the contaminated system. The methods used to communicate information about the spill after the fact do not involve methods directly associated with the actual spill to minimize the risk of further spreading the contamination before such contamination is isolated and eradicated.

RESPONSIBLE PERSONNEL

organization-defined personnel or roles
organization-defined personnel or roles
name: IR-9 (1)

statement

Assign with responsibility for responding to information spills.

guidance

None.
None

TRAINING

organization-defined frequency
organization-defined frequency
name: IR-9 (2)

statement

Provide information spillage response training .

guidance

None.

POST-SPILL OPERATIONS

organization-defined procedures
organization-defined procedures
name: IR-9 (3)

statement

Implement to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions.

guidance

Correction actions for systems contaminated due to information spillages may be very time-consuming. During those periods, personnel may not have access to the contaminated systems, which may potentially affect their ability to conduct organizational business.
None

EXPOSURE TO UNAUTHORIZED PERSONNEL

organization-defined security safeguards
organization-defined security safeguards
name: IR-9 (4)

statement

Employ for personnel exposed to information not within assigned access authorizations.

guidance

Security safeguards include, for example, ensuring that personnel who are exposed to spilled information are made aware of the laws, Executive Orders, directives, regulations, policies, standards, and guidelines regarding the information and the restrictions imposed based on exposure to such information.
None

INTEGRATED INFORMATION SECURITY ANALYSIS TEAM

name: IR-10

statement

Establish an integrated team of forensic and malicious code analysts, tool developers, and real-time operations personnel to handle incidents.

guidance

Having an integrated team for incident response facilitates information sharing. Such capability allows organizational personnel, including developers, implementers, and operators, to leverage the team knowledge of the threat to implement defensive measures that will enable organizations to deter intrusions more effectively. Moreover, integrated teams promote the rapid detection of intrusions, development of appropriate mitigations, and the deployment of effective defensive measures. For example, when an intrusion is detected, the integrated analysis team can rapidly develop an appropriate response for operators to implement, correlate the new incident with information on past intrusions, and augment ongoing intelligence development. This enables the team to identify adversary tactics, techniques, and procedures that are linked to the operations tempo or to specific missions and business functions, and to define responsive actions in a way that does not disrupt those missions and business functions. Information security analysis teams are distributed within organizations to make the capability more resilient.

MAINTENANCE

SYSTEM MAINTENANCE POLICY AND PROCEDURES

organization-defined personnel or roles
organization-defined personnel or roles

organization-defined senior management official
organization-defined senior management official

organization-defined frequency
organization-defined frequency

organization-defined frequency
organization-defined frequency

name: MA-1

statement

item
name: MA-1a.

Develop, document, and disseminate to :

item
name: MA-1a.1.

A system maintenance policy that:

item
name: MA-1a.1.(a)

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

item
name: MA-1a.1.(b)

Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and

item
name: MA-1a.2.

Procedures to facilitate the implementation of the system maintenance policy and the associated system maintenance controls;

item
name: MA-1b.

Designate an to manage the system maintenance policy and procedures;

item
name: MA-1c.

Review and update the current system maintenance:

item
name: MA-1c.1.

Policy ; and

item
name: MA-1c.2.

Procedures ;

item
name: MA-1d.

Ensure that the system maintenance procedures implement the system maintenance policy and controls; and

item
name: MA-1e.

Develop, document, and implement remediation actions for violations of the maintenance policy.

guidance

This control addresses the establishment of policy and procedures for the effective implementation of the controls and control enhancements in the MA family. The risk management strategy is an important factor in establishing policy and procedures. Comprehensive policy and procedures help provide security and privacy assurance. Security and privacy program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general security and privacy policy or can be represented by multiple policies reflecting the complex nature of organizations. The procedures can be established for security and privacy programs and for systems, if needed. Procedures describe how policies or controls are implemented and can be directed at the personnel or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. It is important to recognize that restating controls does not constitute an organizational policy or procedure.

References

NIST Special Publication 800-12
NIST Special Publication 800-30
NIST Special Publication 800-39
NIST Special Publication 800-100

CONTROLLED MAINTENANCE

organization-defined personnel or roles
organization-defined personnel or roles

organization-defined maintenance-related information
organization-defined maintenance-related information
name: MA-2

statement

item
name: MA-2a.

Schedule, document, and review records of maintenance, repair, or replacement on system components in accordance with manufacturer or vendor specifications and/or organizational requirements;

item
name: MA-2b.

Approve and monitor all maintenance activities, whether performed on site or remotely and whether the system or system components are serviced on site or removed to another location;

item
name: MA-2c.

Require that explicitly approve the removal of the system or system components from organizational facilities for off-site maintenance, repair, or replacement;

item
name: MA-2d.

Sanitize equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance, repair, or replacement;

item
name: MA-2e.

Check all potentially impacted security and privacy controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions; and

item
name: MA-2f.

Include in organizational maintenance records.

guidance

This control addresses the information security aspects of the system maintenance program and applies to all types of maintenance to any system component (hardware, firmware, applications) conducted by any local or nonlocal entity. System maintenance also includes those components not directly associated with information processing and/or data or information retention such as scanners, copiers, and printers. Information necessary for creating effective maintenance records includes, for example, date and time of maintenance; name of individuals or group performing the maintenance; name of escort, if necessary; a description of the maintenance performed; and system components or equipment removed or replaced (including identification numbers, if applicable). The level of detail included in maintenance records can be informed by the security

categories of organizational systems. Organizations consider supply chain issues associated with replacement components for systems.

RECORD CONTENT

name: MA-2 (1)

statement

Incorporated into MA-2.

AUTOMATED MAINTENANCE ACTIVITIES

name: MA-2 (2)

statement

item
name: MA-2 (2)(a)

Employ automated mechanisms to schedule, conduct, and document maintenance, repair, and replacement actions for the system or system components; and

item
name: MA-2 (2)(b)

Produce up-to date, accurate, and complete records of all maintenance, repair, and replacement actions requested, scheduled, in process, and completed.

guidance

None.

MAINTENANCE TOOLS

organization-defined frequency
organization-defined frequency
name: MA-3

statement

item
name: MA-3a.

Approve, control, and monitor the use of system maintenance tools; and

item
name: MA-3b.

Review previously approved system maintenance tools .

guidance

This control addresses security-related issues associated with maintenance tools that are not within organizational system boundaries but are used specifically for diagnostic and repair actions on organizational systems. Organizations have flexibility in determining roles for approval of maintenance tools and how that approval is documented. Periodic review of system maintenance tools facilitates withdrawal of the approval for outdated, unsupported, irrelevant, or no-longer-used tools. Maintenance tools can include hardware, software, and firmware items. Maintenance tools are potential vehicles for transporting malicious code, intentionally or unintentionally, into a facility and subsequently into systems. Maintenance tools can include, for example, hardware/software diagnostic test equipment and hardware and software packet sniffers. This control does not cover hardware or software components that support system maintenance and are a part of the system, for example, the software implementing #ping,# #ls,# #ipconfig,# or the hardware and software implementing the monitoring port of an Ethernet switch.

INSPECT TOOLS

name: MA-3 (1)

statement

Inspect the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.

guidance

If, upon inspection of maintenance tools, organizations determine that the tools have been modified in an improper/unauthorized manner or contain malicious code, the incident is handled consistent with organizational policies and procedures for incident handling.

INSPECT MEDIA

name: MA-3 (2)

statement

Check media containing diagnostic and test programs for malicious code before the media are used in the system.

guidance

If, upon inspection of media containing maintenance diagnostic and test programs, organizations determine that the media contain malicious code, the incident is handled consistent with organizational incident handling policies and procedures.

PREVENT UNAUTHORIZED REMOVAL

organization-defined personnel or roles
organization-defined personnel or roles

name: MA-3 (3)

statement

Prevent the removal of maintenance equipment containing organizational information by:

item
name: MA-3 (3)(a)

Verifying that there is no organizational information contained on the equipment;

item
name: MA-3 (3)(b)

Sanitizing or destroying the equipment;

item
name: MA-3 (3)(c)

Retaining the equipment within the facility; or

item
name: MA-3 (3)(d)

Obtaining an exemption from explicitly authorizing removal of the equipment from the facility.

guidance

Organizational information includes all information specifically owned by organizations and information provided to organizations in which organizations serve as information stewards.

RESTRICTED TOOL USE

name: MA-3 (4)

statement

Restrict the use of maintenance tools to authorized personnel only.

guidance

This control enhancement applies to systems that are used to carry out maintenance functions.

References

NIST Special Publication 800-88

NONLOCAL MAINTENANCE

name: MA-4

statement

item
name: MA-4a.

Approve and monitor nonlocal maintenance and diagnostic activities;

item
name: MA-4b.

Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system;

item
name: MA-4c.

Employ strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions;

item
name: MA-4d.

Maintain records for nonlocal maintenance and diagnostic activities; and

item
name: MA-4e.

Terminate session and network connections when nonlocal maintenance is completed.

guidance

Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through a network, either an external network or an internal network. Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the system or system component and not communicating across a network connection. Authentication techniques used in the establishment of nonlocal maintenance and diagnostic sessions reflect the network access requirements in IA-2. Strong authentication requires authenticators that are resistant to replay attacks and employ multifactor authentication. Strong authenticators include, for example, PKI where certificates are stored on a token protected by a password, passphrase, or biometric. Enforcing requirements in MA-4 is accomplished in part by other controls.

AUDITING AND REVIEW

organization-defined audit events
organization-defined audit events
name: MA-4 (1)

statement

item
name: MA-4 (1)(a)

Audit for nonlocal maintenance and diagnostic sessions; and

item
name: MA-4 (1)(b)

Review the records of the maintenance and diagnostic sessions.

guidance

None.

DOCUMENT NONLOCAL MAINTENANCE

name: MA-4 (2)

statement

Incorporated into MA-1 and MA-4

COMPARABLE SECURITY AND SANITIZATION

name: MA-4 (3)

statement

item
name: MA-4 (3)(a)

Require that nonlocal maintenance and diagnostic services be performed from a system that implements a security capability comparable to the capability implemented on the system being serviced; or

item
name: MA-4 (3)(b)

Remove the component to be serviced from the system prior to nonlocal maintenance or diagnostic services; sanitize the component (for organizational information) before removal from organizational facilities; and after the service is performed, inspect and sanitize the component (for potentially malicious software) before reconnecting the component to the system.

guidance

Comparable security capability on systems, diagnostic tools, and equipment providing maintenance services implies that the implemented security controls on those systems, tools, and equipment are at least as comprehensive as the controls on the system being serviced.

AUTHENTICATION AND SEPARATION OF MAINTENANCE SESSIONS

organization-defined authenticators that are replay resistant
organization-defined authenticators that are replay resistant
name: MA-4 (4)

statement

Protect nonlocal maintenance sessions by:

item
name: MA-4 (4)(a)

Employing ; and

item
name: MA-4 (4)(b)

Separating the maintenance sessions from other network sessions with the system by either:

item
name: MA-4 (4)(b)(1)

Physically separated communications paths; or

item
name: MA-4 (4)(b)(2)

Logically separated communications paths based upon encryption.

guidance

None.
None

APPROVALS AND NOTIFICATIONS

organization-defined personnel or roles
organization-defined personnel or roles

organization-defined personnel or roles
organization-defined personnel or roles
name: MA-4 (5)

statement

item

name: MA-4 (5)(a)

Require the approval of each nonlocal maintenance session by ; and

item
name: MA-4 (5)(b)

Notify of the date and time of planned nonlocal maintenance.

guidance

Notification may be performed by maintenance personnel. Approval of nonlocal maintenance sessions is accomplished by organizational personnel with sufficient information security and system knowledge to determine the appropriateness of the proposed maintenance.
None

CRYPTOGRAPHIC PROTECTION

name: MA-4 (6)

statement

Implement cryptographic mechanisms to protect the integrity and confidentiality of nonlocal maintenance and diagnostic communications.

guidance

None.

REMOTE DISCONNECT VERIFICATION

name: MA-4 (7)

statement

Implement remote disconnect verification at the termination of nonlocal maintenance and diagnostic sessions.

guidance

Remote disconnect verification ensures that remote connections from nonlocal maintenance sessions have been terminated and are no longer available for use.

References

FIPS Publication 140-2
FIPS Publication 197
FIPS Publication 201
NIST Special Publication 800-63
NIST Special Publication 800-88

MAINTENANCE PERSONNEL

name: MA-5

statement

item
name: MA-5a.

Establish a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel;

item
name: MA-5b.

Verify that non-escorted personnel performing maintenance on the system possess the required access authorizations; and

item
name: MA-5c.

Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

guidance

This control applies to individuals performing hardware or software maintenance on organizational systems, while PE-2 addresses physical access for individuals whose maintenance duties place them within the physical protection perimeter of the systems. Technical competence of supervising individuals relates to the maintenance performed on the systems while having required access authorizations refers to maintenance on and near the systems. Individuals not previously identified as authorized maintenance personnel, such as information technology manufacturers, vendors, systems integrators, and consultants, may require privileged access to organizational systems, for example, when required to conduct maintenance activities with little or no notice. Based on organizational assessments of risk, organizations may issue temporary credentials to these individuals. Temporary credentials may be for one-time use or for very limited time-periods.

INDIVIDUALS WITHOUT APPROPRIATE ACCESS

name: MA-5 (1)

statement

item
name: MA-5 (1)(a)

Implement procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements:

item
name: MA-5 (1)(a)(1)

Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified;

item
name: MA-5 (1)(a)(2)

Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and

item
name: MA-5 (1)(b)

Develop and implement alternate security safeguards in the event a system component cannot be sanitized, removed, or disconnected from the system.

guidance

This control enhancement denies individuals who lack appropriate security clearances or who are not U.S. citizens, visual and electronic access to any classified or controlled unclassified information contained on organizational systems. Procedures for the use of maintenance personnel can be documented in security plans for the systems.

SECURITY CLEARANCES FOR CLASSIFIED SYSTEMS

name: MA-5 (2)

statement

Verify that personnel performing maintenance and diagnostic activities on a system processing, storing, or transmitting classified information possess security clearances and formal access approvals for at least the highest classification level and for all compartments of information on the system.

guidance

None.

CITIZENSHIP REQUIREMENTS FOR CLASSIFIED SYSTEMS

name: MA-5 (3)

statement

Verify that personnel performing maintenance and diagnostic activities on a system processing, storing, or transmitting classified information are U.S. citizens.

guidance

None.

FOREIGN NATIONALS

name: MA-5 (4)

statement

Verify that:

item
name: MA-5 (4)(a)

Foreign nationals with appropriate security clearances are used to conduct maintenance and diagnostic activities on classified systems only when the systems are jointly owned and operated by the United States and foreign allied governments, or owned and operated solely by foreign allied governments; and

item
name: MA-5 (4)(b)

Approvals, consents, and detailed operational conditions regarding the use of foreign nationals to conduct maintenance and diagnostic activities on classified systems are fully documented within Memoranda of Agreements.

guidance

None.

NON-SYSTEM MAINTENANCE

name: MA-5 (5)

statement

Verify that non-escorted personnel performing maintenance activities not directly associated with the system but in the physical proximity of the system, have required access authorizations.

guidance

Personnel performing maintenance activities in other capacities not directly related to the system include, for example, physical plant personnel and janitorial personnel.
None

TIMELY MAINTENANCE

organization-defined system components
organization-defined system components

organization-defined time-period
organization-defined time-period
name: MA-6

statement

Obtain maintenance support and/or spare parts for within of failure.

guidance

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

PREVENTIVE MAINTENANCE

organization-defined system components
organization-defined system components

organization-defined time intervals
organization-defined time intervals
name: MA-6 (1)

statement

Perform preventive maintenance on at .

guidance

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

None

PREDICTIVE MAINTENANCE

organization-defined system components
organization-defined system components

organization-defined time intervals
organization-defined time intervals

name: MA-6 (2)

statement

Perform predictive maintenance on at .

guidance

Predictive maintenance, or condition-based maintenance, attempts to evaluate the condition of equipment by performing periodic or continuous (online) equipment condition monitoring. The goal of predictive maintenance is to perform maintenance at a scheduled point in time when the maintenance activity is most cost-effective and before the equipment loses performance within a threshold. The predictive component of predictive maintenance stems from the goal of predicting the future trend of the equipment's condition. This approach uses principles of statistical process control to determine at what point in the future maintenance activities will be appropriate. Most predictive maintenance inspections are performed while equipment is in service, thereby minimizing disruption of normal system operations. Predictive maintenance can result in substantial cost savings and higher system reliability. Predictive maintenance tends to include measurement of the item. To evaluate equipment condition, predictive maintenance utilizes nondestructive testing technologies such as infrared, acoustic (partial discharge and airborne ultrasonic), corona detection, vibration analysis, sound level measurements, oil analysis, and other specific online tests.

None

AUTOMATED SUPPORT FOR PREDICTIVE MAINTENANCE

name: MA-6 (3)

statement

Employ automated mechanisms to transfer predictive maintenance data to a computerized maintenance management system.

guidance

A computerized maintenance management system maintains a database of information about the maintenance operations of organizations and automates processing equipment condition data to trigger maintenance planning, execution, and reporting.

None

ADEQUATE SUPPLY

organization-defined security safeguards
organization-defined security safeguards

organization-defined critical system components
organization-defined critical system components
name: MA-6 (4)

statement

Employ to ensure an adequate supply of .

guidance

Adversaries can attempt to impede organizational operations by disrupting the supply of critical system components or corrupting supplier operations. Organizations may track systems and component mean time to failure to mitigate the loss of temporary or permanent system function. Safeguards to ensure that adequate supplies of critical system components include, for example, the use of multiple suppliers throughout the supply chain for the identified critical components; stockpiling spare components to ensure operation during mission-critical times, and the identification of functionally-identical or similar components which may be used, if necessary.

MEDIA PROTECTION

MEDIA PROTECTION POLICY AND PROCEDURES

organization-defined personnel or roles
organization-defined personnel or roles

organization-defined senior management official
organization-defined senior management official

organization-defined frequency
organization-defined frequency

organization-defined frequency
organization-defined frequency
name: MP-1

statement

item
name: MP-1a.

Develop, document, and disseminate to :

item
name: MP-1a.1.

A media protection policy that:

item
name: MP-1a.1.(a)

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

item
name: MP-1a.1.(b)

Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and

item
name: MP-1a.2.

Procedures to facilitate the implementation of the media protection policy and the associated media protection controls;

item
name: MP-1b.

Designate an to manage the media protection policy and procedures;

item
name: MP-1c.

Review and update the current media protection:

item
name: MP-1c.1.

Policy ; and

item
name: MP-1c.2.

Procedures ;

item
name: MP-1d.

Ensure that the media protection procedures implement the media protection policy and controls; and

item
name: MP-1e.

Develop, document, and implement remediation actions for violations of the media protection policy.

guidance

This control addresses the establishment of policy and procedures for the effective implementation of the controls and control enhancements in the MP family. The risk management strategy is an important factor in establishing policy and procedures. Comprehensive policy and procedures help provide security and privacy assurance. Security and privacy program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general security and privacy policy or can be represented by multiple policies reflecting the complex nature of organizations. The procedures can be established for security and privacy programs and for systems, if needed. Procedures describe how policies or controls are implemented and can be directed at the personnel or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. It is important to recognize that restating controls does not constitute an organizational policy or procedure.

References
NIST Special Publication 800-12
NIST Special Publication 800-30
NIST Special Publication 800-39
NIST Special Publication 800-100

MEDIA ACCESS

organization-defined types of digital and/or non-digital media
organization-defined types of digital and/or non-digital media

organization-defined personnel or roles
organization-defined personnel or roles
name: MP-2

statement

Restrict access to to .

guidance

System media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and

digital video disks. Non-digital media includes, for example, paper and microfilm. Restricting non-digital media access includes, for example, denying access to patient medical records in a community hospital unless the individuals seeking access to such records are authorized healthcare providers. Restricting access to digital media includes, for example, limiting access to design specifications stored on compact disks in the media library to the project leader and the individuals on the development team.

AUTOMATED RESTRICTED ACCESS

name: MP-2 (1)
MP-4(2)

statement

Incorporated into MP-4(2).

CRYPTOGRAPHIC PROTECTION

name: MP-2 (2)
SC-28(1)

statement

Incorporated into SC-28(1).

References

FIPS Publication 199
NIST Special Publication 800-111

MEDIA MARKING

organization-defined types of system media
organization-defined types of system media

organization-defined controlled areas
organization-defined controlled areas
name: MP-3

statement

item
name: MP-3a.

Mark system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and

item
name: MP-3b.

Exempt from marking if the media remain within .

guidance

Security marking refers to the application or use of human-readable security attributes. Security labeling refers to the application or use of security attributes regarding internal data structures within systems. System media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external or removable disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Security marking is generally not required for media containing information determined by organizations to be in the public domain or to be publicly releasable. However, some organizations may require markings for public information indicating that the information is publicly releasable. Marking of system media reflects applicable laws, Executive Orders, directives, policies, regulations, standards, and guidelines.

References

FIPS Publication 199

MEDIA STORAGE

organization-defined types of digital and/or non-digital media
organization-defined types of digital and/or non-digital media

organization-defined controlled areas
organization-defined controlled areas
name: MP-4

statement

item
name: MP-4a.

Physically control and securely store within ; and

item
name: MP-4b.

Protect system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

guidance

System media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external or removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm.

Physically controlling system media includes, for example, conducting inventories, ensuring procedures are in place to allow individuals to check out and return media to the media library, and maintaining accountability for stored media. Secure storage includes, for example, a locked drawer, desk, or cabinet; or a controlled media library. The type of media storage employed by organizations is commensurate with the security category or classification of the information residing on the media. Controlled areas are areas that provide sufficient physical and procedural safeguards to meet the requirements established for protecting information and systems. For media containing information determined to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on organizations or individuals if accessed by other than authorized personnel, fewer safeguards may be needed. In these situations, physical access controls provide adequate protection.

CRYPTOGRAPHIC PROTECTION

name: MP-4 (1)
SC-28(1)

statement

Incorporated into SC-28(1).

AUTOMATED RESTRICTED ACCESS

name: MP-4 (2)

statement

Employ automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted.

guidance

Automated mechanisms can include, for example, keypads or card readers on the external entries to media storage areas.

References

FIPS Publication 199
NIST Special Publication 800-111

MEDIA TRANSPORT

organization-defined types of system media
organization-defined types of system media

organization-defined security safeguards
organization-defined security safeguards
name: MP-5

statement

item
name: MP-5a.

Protect and control during transport outside of controlled areas using ;

item
name: MP-5b.

Maintain accountability for system media during transport outside of controlled areas;

item
name: MP-5c.

Document activities associated with the transport of system media; and

item
name: MP-5d.

Restrict the activities associated with the transport of system media to authorized personnel.

guidance

System media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, microfilm and paper. Controlled areas are areas or spaces for which organizations provide sufficient physical or procedural safeguards to meet requirements established for protecting information and systems. Physical and technical safeguards for media are commensurate with the security category or classification of the information residing on the media. Safeguards to protect media during transport include, for example, locked containers and cryptography. Cryptographic mechanisms can provide confidentiality and integrity protections depending upon the mechanisms used. Activities associated with transport include the actual transport as well as those activities such as releasing media for transport and ensuring that media enters the appropriate transport processes. For the actual transport, authorized transport and courier personnel may include individuals from outside the organization. Maintaining accountability of media during transport includes, for example, restricting transport activities to authorized personnel, and tracking and/or obtaining explicit records of transport activities as the media moves through the transportation system to prevent and detect loss, destruction, or tampering. Organizations establish documentation requirements for activities associated with the transport of system media in accordance with organizational assessments of risk to include the flexibility to define different record-keeping methods for the different types of media transport as part of an overall system of transport-related records.

PROTECTION OUTSIDE OF CONTROLLED AREAS

name: MP-5 (1)

statement

Incorporated into MP-5.

DOCUMENTATION OF ACTIVITIES

name: MP-5 (2)

statement

Incorporated into MP-5.

CUSTODIANS

name: MP-5 (3)

statement

Employ an identified custodian during transport of system media outside of controlled areas.

guidance

Identified custodians provide organizations with specific points of contact during the media transport process and facilitate individual accountability. Custodial responsibilities can be transferred from one individual to another if an unambiguous custodian is identified at all times.
None

CRYPTOGRAPHIC PROTECTION

name: MP-5 (4)
SC-28(1)

statement

Incorporated into SC-28(1).

References
FIPS Publication 199

MEDIA SANITIZATION

organization-defined system media
organization-defined system media

organization-defined sanitization techniques and procedures
organization-defined sanitization techniques and procedures
name: MP-6

statement

item

name: MP-6a.

Sanitize prior to disposal, release out of organizational control, or release for reuse using ; and

item
name: MP-6b.

Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

guidance

This control applies to all system media, both digital and non-digital, subject to disposal or reuse, whether or not the media is considered removable. Examples include: digital media found in scanners, copiers, printers, notebook computers, workstations, network components, mobile devices; and non-digital media such as paper and microfilm. The sanitization process removes information from the media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erase, and destruction, prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal. Organizations determine the appropriate sanitization methods recognizing that destruction is sometimes necessary when other methods cannot be applied to media requiring sanitization. Organizations use discretion on the employment of approved sanitization techniques and procedures for media containing information deemed to be in the public domain or publicly releasable, or deemed to have no adverse impact on organizations or individuals if released for reuse or disposal. Sanitization of non-digital media includes, for example, destruction, removing a classified appendix from an otherwise unclassified document, or redacting selected sections or words from a document by obscuring the redacted sections or words in a manner equivalent in effectiveness to removing them from the document. NARA policy and guidance control the sanitization process for controlled unclassified information. NSA standards and policies control the sanitization process for media containing classified information.

REVIEW, APPROVE, TRACK, DOCUMENT, AND VERIFY

name: MP-6 (1)

statement

Review, approve, track, document, and verify media sanitization and disposal actions.

guidance

Organizations review and approve media to be sanitized to ensure compliance with records-retention policies. Tracking and documenting actions include, for example, listing personnel who reviewed and approved sanitization and disposal actions; types of media sanitized; specific files stored on the media; sanitization methods used; date and time of the sanitization actions; personnel who performed the sanitization; verification actions taken; personnel who performed

the verification; and the disposal actions taken. Organizations verify that the sanitization of the media was effective prior to disposal.
None

EQUIPMENT TESTING

organization-defined frequency
organization-defined frequency
name: MP-6 (2)

statement

Test sanitization equipment and procedures to verify that the intended sanitization is being achieved.

guidance

Testing of sanitization equipment and procedures may be conducted by qualified and authorized external entities including, for example, federal agencies or external service providers.
None

NONDESTRUCTIVE TECHNIQUES

organization-defined circumstances requiring sanitization of portable storage devices
organization-defined circumstances requiring sanitization of portable storage devices
name: MP-6 (3)

statement

Apply nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the system under the following circumstances: .

guidance

Portable storage devices can be the source of malicious code insertions into organizational systems. Many of these devices are obtained from untrustworthy sources and may contain malicious code that can be readily transferred to systems through USB ports or other entry portals. While scanning storage devices is recommended, sanitization provides additional assurance that such devices are free of malicious code. Organizations consider nondestructive sanitization of portable storage devices when these devices are purchased from manufacturers or vendors prior to initial use or when organizations cannot maintain a positive chain of custody for the devices.
None

CONTROLLED UNCLASSIFIED INFORMATION

name: MP-6 (4)

statement

Incorporated into MP-6.

CLASSIFIED INFORMATION

name: MP-6 (5)

statement

Incorporated into MP-6.

MEDIA DESTRUCTION

name: MP-6 (6)

statement

Incorporated into MP-6.

DUAL AUTHORIZATION

organization-defined system media
organization-defined system media
name: MP-6 (7)

statement

Enforce dual authorization for the sanitization of .

guidance

Organizations employ dual authorization to ensure that system media sanitization cannot occur unless two technically qualified individuals conduct the designated task. Individuals sanitizing system media possess sufficient skills and expertise to determine if the proposed sanitization reflects applicable federal and organizational standards, policies, and procedures. Dual authorization also helps to ensure that sanitization occurs as intended, both protecting against errors and false claims of having performed the sanitization actions. Dual authorization may also be known as two-person control.

REMOTE PURGING OR WIPING OF INFORMATION

organization-defined systems or system components
organization-defined systems or system components

organization-defined conditions
organization-defined conditions
name: MP-6 (8)

statement

Provide the capability to purge or wipe information from either remotely or under the following conditions: .

guidance

This control enhancement protects data/information on organizational systems and system components if such systems or components are obtained by unauthorized individuals. Remote purge/wipe commands require strong authentication to mitigate the risk of unauthorized individuals purging/wiping the system/component/device. The purge or wipe function can be implemented in a variety of ways including, for example, by overwriting data/information multiple times or by destroying the key necessary to decrypt encrypted data.
None

DESTRUCTION OF PERSONALLY IDENTIFIABLE INFORMATION

name: MP-6 (9)

statement

Facilitate the destruction of personally identifiable information by:

item
name: MP-6 (9)(a)

De-identifying the personally identifiable information;

item
name: MP-6 (9)(b)

Proactively reviewing media to actively find personally identifiable information and removing such information; and

item
name: MP-6 (9)(c)

Reviewing media as it is being archived or disposed to find and remove personally identifiable information.

guidance

Disposal or destruction of media containing personally identifiable information applies to originals, copies, and archived records, including system logs that may contain such information. De-identification is the general term for any process of removing the association between a set of identifying data and the data subject and is accomplished in a manner that prevents loss, theft, misuse, or unauthorized access.

References

FIPS Publication 199
NIST Special Publication 800-88
NIST Special Publication 800-124

MEDIA USE

organization-defined types of system media
organization-defined types of system media

organization-defined systems or system components
organization-defined systems or system components

organization-defined security safeguards
organization-defined security safeguards
name: MP-7

statement

item
name: MP-7a.

[Selection: Restrict; Prohibit] the use of on using ; and

item
name: MP-7b.

Prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner.

guidance

System media includes digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external or removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. This control also applies to mobile devices with information storage capability. In contrast to MP-2, which restricts user access to media, this control restricts the use of certain types of media on systems, for example, restricting/prohibiting the use of flash drives or external hard disk drives. Organizations can employ technical and nontechnical safeguards to restrict the use of system media. Organizations may restrict the use of portable storage devices, for example, by using physical cages on workstations to prohibit access to certain external ports, or disabling or removing the ability to insert, read or write to such devices. Organizations may also limit the use of portable storage devices to only approved devices including, for example, devices provided by the organization, devices provided by other approved organizations, and devices that are not personally owned. Finally, organizations may restrict the use of portable storage devices based on the type of device, for example, prohibiting the use of writeable, portable storage devices, and implementing this restriction by disabling or removing the capability to write to such devices. Requiring identifiable owners for portable storage devices reduces the risk of using such devices by allowing organizations to assign responsibility for addressing known vulnerabilities in the devices.

PROHIBIT USE WITHOUT OWNER

name: MP-7 (1)

statement

Incorporated into MP-7.

PROHIBIT USE OF SANITIZATION-RESISTANT MEDIA

name: MP-7 (2)

statement

Prohibit the use of sanitization-resistant media in organizational systems.

guidance

Sanitization-resistance refers to non-destructive sanitization techniques and applies to the capability to purge information from media. Certain types of media do not support sanitize commands, or if supported, the interfaces are not supported in a standardized way across these devices. Sanitization-resistant media include, for example, compact flash, embedded flash on boards and devices, solid state drives, and USB removable media.

References

FIPS Publication 199
NIST Special Publication 800-111

MEDIA DOWNGRADING

organization-defined system media downgrading process
organization-defined system media downgrading process

organization-defined system media requiring downgrading
organization-defined system media requiring downgrading

name: MP-8

statement

item

name: MP-8a.

Establish that includes employing downgrading mechanisms with strength and integrity commensurate with the security category or classification of the information;

item

name: MP-8b.

Verify that the system media downgrading process is commensurate with the security category and/or classification level of the information to be removed and the access authorizations of the potential recipients of the downgraded information;

item
name: MP-8c.

Identify ; and

item
name: MP-8d.

Downgrade the identified system media using the established process.

guidance

This control applies to all system media, digital and non-digital, subject to release outside of the organization, whether the media is considered removable or not removeable. The downgrading process, when applied to system media, removes information from the media, typically by security category or classification level, such that the information cannot be retrieved or reconstructed. Downgrading of media includes redacting information to enable wider release and distribution. It also ensures that empty space on the media is devoid of information.

DOCUMENTATION OF PROCESS

name: MP-8 (1)

statement

Document system media downgrading actions.

guidance

Organizations can document the media downgrading process by providing information such as the downgrading technique employed, the identification number of the downgraded media, and the identity of the individual that authorized and/or performed the downgrading action.
None

EQUIPMENT TESTING

organization-defined frequency
organization-defined frequency
name: MP-8 (2)

statement

Test downgrading equipment and procedures to verify that intended downgrading actions are being achieved.

guidance

None.
None

CONTROLLED UNCLASSIFIED INFORMATION

organization-defined Controlled Unclassified Information (CUI)
organization-defined Controlled Unclassified Information (CUI)
name: MP-8 (3)

statement

Downgrade system media containing prior to public release.

guidance

None.
None

CLASSIFIED INFORMATION

name: MP-8 (4)

statement

Downgrade system media containing classified information prior to release to individuals without required access authorizations.

guidance

Downgrading of classified information uses approved sanitization tools, techniques, and procedures to transfer information confirmed to be unclassified from classified systems to unclassified media.
None

PRIVACY AUTHORIZATION

PRIVACY AUTHORIZATION POLICY AND PROCEDURES

organization-defined personnel or roles
organization-defined personnel or roles

organization-defined senior management official
organization-defined senior management official

organization-defined frequency
organization-defined frequency

organization-defined frequency
organization-defined frequency

name: PA-1

statement

item
name: PA-1a.

Develop, document, and disseminate to :

item
name: PA-1a.1.

A privacy authorization policy that:

item
name: PA-1a.1.(a)

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

item
name: PA-1a.1.(b)

Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and

item
name: PA-1a.2.

Procedures to facilitate the implementation of the privacy authorization policy and the associated privacy authorization controls;

item
name: PA-1b.

Designate an to manage the privacy authorization policy and procedures;

item
name: PA-1c.

Review and update the current privacy authorization:

item
name: PA-1c.1.

Policy ; and

item
name: PA-1c.2.

Procedures ;

item
name: PA-1d.

Ensure that the privacy authorization procedures implement the privacy authorization policy and controls; and

item
name: PA-1e.

Develop, document, and implement remediation actions for violations of the privacy authorization policy.

guidance

This control addresses the establishment of policy and procedures for the effective implementation of the controls and control enhancements in the PA family. The risk management strategy is an important factor in establishing policy and procedures. Comprehensive policy and procedures help provide security and privacy assurance. Security and privacy program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general security and privacy policy or can be represented by multiple policies reflecting the complex nature of organizations. The procedures can be established for security and privacy programs and for systems, if needed. Procedures describe how policies or controls are implemented and can be directed at the personnel or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. It is important to recognize that restating controls does not constitute an organizational policy or procedure.

References

NIST Special Publication 800-12
NIST Special Publication 800-30
NIST Special Publication 800-39
NIST Special Publication 800-100

AUTHORITY TO COLLECT

name: PA-2

statement

Determine and document the legal authority that permits the collection, use, maintenance, and sharing of personally identifiable information, either generally or in support of a specific program or system need.

guidance

Prior to collecting personally identifiable information, organizations determine whether the collection of such information is legally authorized. Organizational officials consult with the Senior Agency Official for Privacy and legal counsel regarding the authority of any program or activity to collect personally identifiable information. The authority to collect personally identifiable information is documented in the System of Records Notice and/or Privacy Impact Assessment or other applicable documentation such as Privacy Act Statements or Computer Matching Agreements.

PURPOSE SPECIFICATION

name: PA-3

statement

Identify and document the purpose(s) for which personally identifiable information is collected, used, maintained, and shared in its privacy notices.

guidance

Statutory language often expressly authorizes specific collections and uses of personally identifiable information. When statutory language is written broadly and thus subject to interpretation, organizations consult with the Senior Agency Official for Privacy and legal counsel to verify that there is a close nexus between the general authorization and any specific collection of personally identifiable information. Once the specific purpose has been identified, the purpose is clearly described in the related privacy compliance documentation, including, for example, Privacy Impact Assessments, System of Records Notices, and Privacy Act Statements provided at the time of collection including, for example, on forms organizations use to collect personally identifiable information. Further, in order to avoid unauthorized collections or uses of personally identifiable information, personnel who manage such information receive role-based training as specified in AT-3.

USAGE RESTRICTIONS OF PERSONALLY IDENTIFIABLE INFORMATION

name: PA-3 (1)

statement

Restrict the use of personally identifiable information to only the authorized purpose(s) consistent with applicable laws or regulations and/or in public notices.

guidance

Organizations take steps to help ensure that personally identifiable information is used only for legally authorized purposes and in a manner, compatible with the uses identified in the Privacy Act and/or in public notices. These steps include, for example, monitoring and auditing organizational use of personally identifiable information and training organizational personnel

on the authorized uses of such information. With guidance from the Senior Agency Official for Privacy and where appropriate, legal counsel, organizations document the processes and procedures for evaluating the proposed new uses of personally identifiable information to assess whether such uses fall within the scope of the organizational authorities. Where appropriate, organizations obtain consent from individuals for the new uses of personally identifiable information.
None

AUTOMATION

name: PA-3 (2)

statement

Employ automated mechanisms to support records management of authorizing policies and procedures for personally identifiable information.

guidance

Automated mechanisms may be used to support records management of authorizing policies and procedures for personally identifiable information. Automated mechanisms augment verification that organizational policies and procedures are enforced for the management and tracking of personally identifiable information within an organization#s systems.

INFORMATION SHARING WITH EXTERNAL PARTIES

organization-defined personnel or roles
organization-defined personnel or roles
name: PA-4

statement

item

name: PA-4a.

Develop, document, and disseminate guidelines to for the sharing of personally identifiable information externally, only for the authorized purposes identified in the Privacy Act and/or described in its notices, or for a purpose that is compatible with those purposes;

item

name: PA-4b.

Evaluate proposed new instances of sharing personally identifiable information with external parties to assess whether:

item

name: PA-4b.1.

The sharing is authorized; and

item
name: PA-4b.2.

Additional or new public notice is required;

item
name: PA-4c.

Enter into information sharing agreements with external parties that specifically:

item
name: PA-4c.1.

Describe the personally identifiable information covered;

item
name: PA-4c.2.

Enumerate the purpose(s) for which the personally identifiable information may be used; and

item
name: PA-4c.3.

Include security requirements consistent with the information being shared; and

item
name: PA-4d.

Monitor and audit the authorized sharing of personally identifiable information with external parties.

guidance

The Senior Agency Official for Privacy and where appropriate, legal counsel, review and approve proposed external sharing of personally identifiable information, including with other public, international, or private sector entities, for consistency with the uses described in the existing organizational public notice(s). Formal agreements for information sharing include, for example, Memoranda of Understanding, Letters of Intent, Memoranda of Agreement, and Computer Matching Agreements. When a proposed new instance of external sharing of personally identifiable information is not currently authorized by the Privacy Act and/or specified in a notice, organizations evaluate whether the proposed external sharing is compatible with the purpose(s) specified in the notice. If the proposed sharing is compatible, organizations review, update, and republish the Privacy Impact Assessments, System of Records Notices, website privacy policies, and other public notices, if any, to include specific descriptions of the new use(s) and obtain consent where appropriate and feasible.

PHYSICAL AND ENVIRONMENTAL PROTECTION

PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES

organization-defined personnel or roles
organization-defined personnel or roles

organization-defined senior management official
organization-defined senior management official

organization-defined frequency
organization-defined frequency

organization-defined frequency
organization-defined frequency
name: PE-1

statement

item
name: PE-1a.

Develop, document, and disseminate to :

item
name: PE-1a.1.

A physical and environmental protection policy that:

item
name: PE-1a.1.(a)

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

item
name: PE-1a.1.(b)

Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and

item
name: PE-1a.2.

Procedures to facilitate the implementation of the physical and environmental protection policy and the associated physical and environmental protection controls;

item
name: PE-1b.

Designate an to manage the physical and environmental protection policy and procedures;

item
name: PE-1c.

Review and update the current physical and environmental protection:

item
name: PE-1c.1.

Policy ; and

item
name: PE-1c.2.

Procedures ;

item
name: PE-1d.

Ensure that the physical and environmental protection procedures implement the physical and environmental protection policy and controls; and

item
name: PE-1e.

Develop, document, and implement remediation actions for violations of the physical and environmental protection policy.

guidance

This control addresses the establishment of policy and procedures for the effective implementation of the controls and control enhancements in the PE family. The risk management strategy is an important factor in establishing policy and procedures. Comprehensive policy and procedures help provide security and privacy assurance. Security and privacy program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general security and privacy policy or can be represented by multiple policies reflecting the complex nature of organizations. The procedures can be established for security and privacy programs and for systems, if needed. Procedures describe how policies or controls are implemented and can be directed at the personnel or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. It is important to recognize that restating controls does not constitute an organizational policy or procedure.

References

NIST Special Publication 800-12
NIST Special Publication 800-30
NIST Special Publication 800-39
NIST Special Publication 800-100

PHYSICAL ACCESS AUTHORIZATIONS

organization-defined frequency
organization-defined frequency
name: PE-2

statement

item
name: PE-2a.

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

item
name: PE-2b.

Issue authorization credentials for facility access;

item
name: PE-2c.

Review the access list detailing authorized facility access by individuals ; and

item
name: PE-2d.

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

guidance

This control applies to employees and visitors. Individuals with permanent physical access authorization credentials are not considered visitors. Authorization credentials include, for example, badges, identification cards, and smart cards. Organizations determine the strength of authorization credentials needed consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines. This control only applies to areas within facilities that have not been designated as publicly accessible.

ACCESS BY POSITION OR ROLE

name: PE-2 (1)

statement

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

guidance

None.

TWO FORMS OF IDENTIFICATION

organization-defined list of acceptable forms of identification
organization-defined list of acceptable forms of identification
name: PE-2 (2)

statement

Require two forms of identification from for visitor access to the facility where the system resides.

guidance

Acceptable forms of identification include, for example, passports, Personal Identity Verification (PIV) cards, and drivers# licenses. For gaining access to facilities using automated mechanisms, organizations may use PIV cards, key cards, PINs, and biometrics.

RESTRICT UNESCORTED ACCESS

organization-defined credentials
organization-defined credentials
name: PE-2 (3)

statement

Restrict unescorted access to the facility where the system resides to personnel with [Selection (one or more): security clearances for all information contained within the system; formal access authorizations for all information contained within the system; need for access to all information contained within the system;].

guidance

Due to the highly sensitive nature of classified information stored within certain facilities, it is important that individuals lacking sufficient security clearances, access approvals, or need to know, be escorted by individuals with appropriate credentials to ensure that such information is not exposed or otherwise compromised.

References

FIPS Publication 201
NIST Special Publication 800-76
NIST Special Publication 800-73
NIST Special Publication 800-78

PHYSICAL ACCESS CONTROL

organization-defined entry and exit points to the facility where the system resides
organization-defined entry and exit points to the facility where the system resides

organization-defined physical access control systems or devices
organization-defined physical access control systems or devices

organization-defined entry/exit points
organization-defined entry/exit points

organization-defined security safeguards
organization-defined security safeguards

organization-defined circumstances requiring visitor escorts and monitoring
organization-defined circumstances requiring visitor escorts and monitoring

organization-defined physical access devices
organization-defined physical access devices

organization-defined frequency
organization-defined frequency

organization-defined frequency
organization-defined frequency
name: PE-3

statement

item
name: PE-3a.

Enforce physical access authorizations at by;

item
name: PE-3a.1.

Verifying individual access authorizations before granting access to the facility; and

item
name: PE-3a.2.

Controlling ingress and egress to the facility using [Selection (one or more): ; guards];

item
name: PE-3b.

Maintain physical access audit logs for ;

item
name: PE-3c.

Provide to control access to areas within the facility designated as publicly accessible;

item
name: PE-3d.

Escort visitors and monitor visitor activity ;

item
name: PE-3e.

Secure keys, combinations, and other physical access devices;

item
name: PE-3f.

Inventory every ; and

item
name: PE-3g.

Change combinations and keys and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.

guidance

This control applies to employees and visitors. Individuals with permanent physical access authorization credentials are not considered visitors. Organizations determine the types of facility guards needed including, for example, professional security staff, administrative staff, or system users. Physical access devices include, for example, keys, locks, combinations, and card readers. Physical access control systems comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidelines. Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural, automated, or some combination thereof. Physical access points can include facility access points, interior access points to systems or system components requiring supplemental access controls, or both. Components of systems may be in areas designated as publicly accessible with organizations safeguarding access to such devices.

SYSTEM ACCESS

organization-defined physical spaces containing one or more components of the system
organization-defined physical spaces containing one or more components of the system
name: PE-3 (1)

statement

Enforce physical access authorizations to the system in addition to the physical access controls for the facility at .

guidance

This control enhancement provides additional physical security for those areas within facilities where there is a concentration of system components.

FACILITY AND SYSTEM BOUNDARIES

organization-defined frequency
organization-defined frequency
name: PE-3 (2)

statement

Perform security checks at the physical boundary of the facility or system for exfiltration of information or removal of system components.

guidance

Organizations determine the extent, frequency, and/or randomness of security checks to adequately mitigate risk associated with exfiltration.

CONTINUOUS GUARDS

organization-defined physical access points
organization-defined physical access points
name: PE-3 (3)

statement

Employ guards to control to the facility where the system resides 24 hours per day, 7 days per week.

guidance

None.

LOCKABLE CASINGS

organization-defined system components
organization-defined system components
name: PE-3 (4)

statement

Use lockable physical casings to protect from unauthorized physical access.

guidance

None.
None

TAMPER PROTECTION

organization-defined security safeguards
organization-defined security safeguards

organization-defined hardware components
organization-defined hardware components

name: PE-3 (5)

statement

Employ to [Selection (one or more): detect; prevent] physical tampering or alteration of within the system.

guidance

Organizations implement tamper detection and prevention at selected hardware components or tamper detection at some components and tamper prevention at other components. Such detection and prevention activities can employ many types of anti-tamper technologies including, for example, tamper-detection seals and anti-tamper coatings. Anti-tamper programs help to detect hardware alterations through counterfeiting and other supply chain-related risks.

FACILITY PENETRATION TESTING

name: PE-3 (6)

statement

Incorporated into CA-8.

PHYSICAL BARRIERS

name: PE-3 (7)

statement

Limit access using physical barriers.

guidance

Physical barriers include, for example, bollards, concrete slabs, jersey walls, and hydraulic active vehicle barriers.
None

References

FIPS Publication 201
NIST Special Publication 800-73
NIST Special Publication 800-76

NIST Special Publication 800-78
NIST Special Publication 800-116

ACCESS CONTROL FOR TRANSMISSION

organization-defined system distribution and transmission lines
organization-defined system distribution and transmission lines

organization-defined security safeguards
organization-defined security safeguards
name: PE-4

statement

Control physical access to within organizational facilities using .

guidance

Security safeguards applied to system distribution and transmission lines prevent accidental damage, disruption, and physical tampering. Such safeguards may also be necessary to help prevent eavesdropping or modification of unencrypted transmissions. Safeguards used to control physical access to system distribution and transmission lines include, for example, locked wiring closets; disconnected or locked spare jacks; protection of cabling by conduit or cable trays; and wiretapping sensors.

ACCESS CONTROL FOR OUTPUT DEVICES

organization-defined output devices
organization-defined output devices
name: PE-5

statement

Control physical access to output from to prevent unauthorized individuals from obtaining the output.

guidance

Controlling physical access to output devices includes, for example, placing output devices in locked rooms or other secured areas and allowing access to authorized individuals only; placing output devices in locations that can be monitored by organizational personnel; installing monitor or screen filters; and using headphones. Output devices include, for example, monitors, printers, copiers, scanners, facsimile machines, and audio devices.

ACCESS TO OUTPUT BY AUTHORIZED INDIVIDUALS

name: PE-5 (1)

statement

Verify that only authorized individuals receive output from output devices.

guidance

Methods to ensure only authorized individuals receive output from output devices include, for example, placing printers, copiers, and facsimile machines in controlled areas with keypad or card reader access controls; and limiting access to individuals with certain types of badges.
None

ACCESS TO OUTPUT BY INDIVIDUAL IDENTITY

name: PE-5 (2)

statement

Link individual identity to receipt of output from output devices.

guidance

Methods to link individual identity to receipt of output from output devices include, for example, installing security functionality on facsimile machines, copiers, and printers. Such functionality allows organizations to implement authentication on output devices prior to the release of output to individuals.
None

MARKING OUTPUT DEVICES

organization-defined system output devices
organization-defined system output devices

name: PE-5 (3)

statement

Mark indicating the appropriate security marking of the information permitted to be output from the device.

guidance

Outputs devices include, for example, printers, monitors, facsimile machines, scanners, copiers, and audio devices.
None

MONITORING PHYSICAL ACCESS

organization-defined frequency
organization-defined frequency

organization-defined events or potential indications of events
organization-defined events or potential indications of events
name: PE-6

statement

item
name: PE-6a.

Monitor physical access to the facility where the system resides to detect and respond to physical security incidents;

item
name: PE-6b.

Review physical access logs and upon occurrence of ; and

item
name: PE-6c.

Coordinate results of reviews and investigations with the organizational incident response capability.

guidance

Monitoring of physical access includes publicly accessible areas within organizational facilities. This can be accomplished for example, by the employment of guards; the use of video surveillance equipment such as cameras; or the use of sensor devices. Organizational incident response capabilities include investigations of and responses to detected physical security incidents. Security incidents include, for example, security violations or suspicious physical access activities. Suspicious physical access activities include, for example, accesses outside of normal work hours; repeated accesses to areas not normally accessed; accesses for unusual lengths of time; and out-of-sequence accesses.

INTRUSION ALARMS AND SURVEILLANCE EQUIPMENT

name: PE-6 (1)

statement

Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment.

guidance

None.
None

AUTOMATED INTRUSION RECOGNITION AND RESPONSES

organization-defined classes or types of intrusions
organization-defined classes or types of intrusions

organization-defined response actions
organization-defined response actions
name: PE-6 (2)

statement

Employ automated mechanisms to recognize and initiate .

guidance

None.

VIDEO SURVEILLANCE

organization-defined operational areas
organization-defined operational areas

organization-defined time-period
organization-defined time-period
name: PE-6 (3)

statement

Employ video surveillance of and retain video recordings for .

guidance

This control enhancement focuses on recording surveillance video for purposes of subsequent review, if circumstances so warrant. It does not require monitoring surveillance video although organizations may choose to do so. Note that there may be legal considerations when performing and retaining video surveillance, especially if such surveillance is in a public location.
None

MONITORING PHYSICAL ACCESS TO SYSTEMS

organization-defined physical spaces containing one or more components of the system
organization-defined physical spaces containing one or more components of the system
name: PE-6 (4)

statement

Monitor physical access to the system in addition to the physical access monitoring of the facility at .

guidance

This control enhancement provides additional monitoring for those areas within facilities where there is a concentration of system components including, for example, server rooms, media storage areas, and communications centers.
None

VISITOR CONTROL

name: PE-7

statement

Incorporated into PE-2 and PE-3.

VISITOR ACCESS RECORDS

organization-defined time-period
organization-defined time-period

organization-defined frequency
organization-defined frequency
name: PE-8

statement

item
name: PE-8a.

Maintain visitor access records to the facility where the system resides for ; and

item
name: PE-8b.

Review visitor access records .

guidance

Visitor access records include, for example, names and organizations of persons visiting; visitor signatures; forms of identification; dates of access; entry and departure times; purpose of visits; and names and organizations of persons visited. Access records are not required for publicly accessible areas.

AUTOMATED RECORDS MAINTENANCE AND REVIEW

name: PE-8 (1)

statement

Employ automated mechanisms to facilitate the maintenance and review of visitor access records.

guidance

None.
None

PHYSICAL ACCESS RECORDS

name: PE-8 (2)

statement

Incorporated into PE-2.

POWER EQUIPMENT AND CABLING

name: PE-9

statement

Protect power equipment and power cabling for the system from damage and destruction.

guidance

Organizations determine the types of protection necessary for the power equipment and cabling employed at different locations both internal and external to organizational facilities and environments of operation. This includes, for example, generators and power cabling outside of buildings; internal cabling and uninterruptable power sources within an office or data center; and power sources for self-contained entities such as vehicles and satellites.

REDUNDANT CABLING

organization-defined distance
organization-defined distance

name: PE-9 (1)

statement

Employ redundant power cabling paths that are physically separated by .

guidance

Physically separate and redundant power cables ensure that power continues to flow in the event one of the cables is cut or otherwise damaged.
None

AUTOMATIC VOLTAGE CONTROLS

organization-defined critical system components
organization-defined critical system components
name: PE-9 (2)

statement

Employ automatic voltage controls for .

guidance

Automatic voltage controls can monitor and control voltage. Such controls include, for example, voltage regulators, voltage conditioners, and voltage stabilizers.
None

EMERGENCY SHUTOFF

organization-defined location by system or system component
organization-defined location by system or system component
name: PE-10

statement

item
name: PE-10a.

Provide the capability of shutting off power to the system or individual system components in emergency situations;

item
name: PE-10b.

Place emergency shutoff switches or devices in to facilitate safe and easy access for personnel; and

item
name: PE-10c.

Protect emergency power shutoff capability from unauthorized activation.

guidance

This control applies primarily to facilities containing concentrations of system resources including, for example, data centers, server rooms, rooms/buildings containing computer-controlled machinery, and mainframe computer rooms.

ACCIDENTAL AND UNAUTHORIZED ACTIVATION

name: PE-10 (1)

statement

Incorporated into PE-10.

EMERGENCY POWER

name: PE-11

statement

Provide a short-term uninterruptible power supply to facilitate [Selection (one or more): an orderly shutdown of the system; transition of the system to long-term alternate power] in the event of a primary power source loss.

guidance

None.

LONG-TERM ALTERNATE POWER SUPPLY # MINIMAL OPERATIONAL CAPABILITY

name: PE-11 (1)

statement

Provide a long-term alternate power supply for the system that can maintain minimally required operational capability in the event of an extended loss of the primary power source.

guidance

This control enhancement can be satisfied, for example, by using a secondary commercial power supply or other external power supply. The long-term alternate power supplies for organizational systems are either manually or automatically activated.
None

LONG-TERM ALTERNATE POWER SUPPLY # SELF-CONTAINED

name: PE-11 (2)

statement

Provide a long-term alternate power supply for the system that is:

item
name: PE-11 (2)(a)

Self-contained;

item
name: PE-11 (2)(b)

Not reliant on external power generation; and

item
name: PE-11 (2)(c)

Capable of maintaining [Selection: minimally required operational capability; full operational capability] in the event of an extended loss of the primary power source.

guidance

This control enhancement can be satisfied, for example, by using one or more generators with sufficient capacity to meet the needs of the organization. Long-term alternate power supplies for organizational systems are either manually or automatically activated.
None

EMERGENCY LIGHTING
name: PE-12

statement

Employ and maintain automatic emergency lighting for the system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

guidance

This control applies primarily to facilities containing concentrations of system resources including, for example, data centers, server rooms, and mainframe computer rooms.

ESSENTIAL MISSIONS AND BUSINESS FUNCTIONS
name: PE-12 (1)

statement

Provide emergency lighting for all areas within the facility supporting essential missions and business functions.

guidance

None.

None

FIRE PROTECTION

name: PE-13

statement

Employ and maintain fire suppression and detection devices/systems for the system that are supported by an independent energy source.

guidance

This control applies primarily to facilities containing concentrations of system resources including, for example, data centers, server rooms, and mainframe computer rooms. Fire suppression and detection devices or systems that may require an independent energy source include, for example, sprinkler systems, fixed fire hoses, and smoke detectors.

DETECTION DEVICES AND SYSTEMS

organization-defined personnel or roles
organization-defined personnel or roles

organization-defined emergency responders
organization-defined emergency responders

name: PE-13 (1)

statement

Employ fire detection devices/systems for the system that activate automatically and notify and in the event of a fire.

guidance

Organizations can identify specific personnel, roles, and emergency responders if individuals on the notification list need to have appropriate access authorizations and/or clearances, for example, to obtain access to facilities where classified operations are taking place or where there are systems containing classified information.

None

AUTOMATIC SUPPRESSION DEVICES AND SYSTEMS

organization-defined personnel or roles
organization-defined personnel or roles

organization-defined emergency responders
organization-defined emergency responders

name: PE-13 (2)

statement

item
name: PE-13 (2)(a)

Employ fire suppression devices/systems for the system that provide automatic notification of any activation to and ; and

item
name: PE-13 (2)(b)

Employ an automatic fire suppression capability for the system when the facility is not staffed on a continuous basis.

guidance

Organizations can identify specific personnel, roles, and emergency responders if individuals on the notification list need to have appropriate access authorizations and/or clearances, for example, to obtain access to facilities where classified operations are taking place or where there are systems containing classified information.
None

AUTOMATIC FIRE SUPPRESSION

name: PE-13 (3)
PE-13(2)

statement

Incorporated into PE-13(2).

INSPECTIONS

organization-defined frequency
organization-defined frequency

organization-defined time-period
organization-defined time-period
name: PE-13 (4)

statement

Verify that the facility undergoes fire protection inspections by authorized and qualified inspectors and resolves identified deficiencies within .

guidance

None.
None

TEMPERATURE AND HUMIDITY CONTROLS

organization-defined acceptable levels
organization-defined acceptable levels

organization-defined frequency
organization-defined frequency
name: PE-14

statement

item
name: PE-14a.

Maintain temperature and humidity levels within the facility where the system resides at ; and

item
name: PE-14b.

Monitor temperature and humidity levels .

guidance

This control applies primarily to facilities containing concentrations of system resources, for example, data centers, server rooms, and mainframe computer rooms.

AUTOMATIC CONTROLS

name: PE-14 (1)

statement

Employs automatic temperature and humidity controls in the facility to prevent fluctuations potentially harmful to the system.

guidance

None.
None

MONITORING WITH ALARMS AND NOTIFICATIONS

organization-defined personnel or roles
organization-defined personnel or roles
name: PE-14 (2)

statement

Employ temperature and humidity monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment to .

guidance

None.
None

WATER DAMAGE PROTECTION

name: PE-15

statement

Protect the system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

guidance

This control applies primarily to facilities containing concentrations of system resources including, for example, data centers, server rooms, and mainframe computer rooms. Isolation valves can be employed in addition to or in lieu of master shutoff valves to shut off water supplies in specific areas of concern, without affecting entire organizations.

AUTOMATION SUPPORT

organization-defined personnel or roles
organization-defined personnel or roles

name: PE-15 (1)

statement

Employ automated mechanisms to detect the presence of water near the system and alert .

guidance

Automated mechanisms include, for example, water detection sensors, alarms, and notification systems.
None

DELIVERY AND REMOVAL

organization-defined types of system components
organization-defined types of system components

name: PE-16

statement

Authorize, monitor, and control entering and exiting the facility and maintain records of those items.

guidance

Enforcing authorizations for entry and exit of system components may require restricting access to delivery areas and isolating the areas from the system and media libraries.

ALTERNATE WORK SITE

organization-defined alternate work sites
organization-defined alternate work sites

organization-defined security and privacy controls
organization-defined security and privacy controls
name: PE-17

statement

item
name: PE-17a.

Determine and document the allowed for use by employees;

item
name: PE-17b.

Employ at alternate work sites;

item
name: PE-17c.

Assess the effectiveness of security and privacy controls at alternate work sites; and

item
name: PE-17d.

Provide a means for employees to communicate with information security and privacy personnel in case of security or privacy incidents or problems.

guidance

Alternate work sites include, for example, government facilities or private residences of employees. While distinct from alternative processing sites, alternate work sites can provide readily available alternate locations during contingency operations. Organizations can define different sets of controls for specific alternate work sites or types of sites depending on the work-related activities conducted at those sites. This control supports the contingency planning activities of organizations.

References

NIST Special Publication 800-46

LOCATION OF SYSTEM COMPONENTS

organization-defined physical and environmental hazards
organization-defined physical and environmental hazards
name: PE-18

statement

Position system components within the facility to minimize potential damage from and to minimize the opportunity for unauthorized access.

guidance

Physical and environmental hazards include, for example, flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electromagnetic pulse, electrical interference, and other forms of incoming electromagnetic radiation. Organizations also consider the location of entry points where unauthorized individuals, while not being granted access, might nonetheless be near systems. Such proximity can increase the risk of unauthorized access to organizational communications, including, for example, using wireless sniffers or microphones.

FACILITY SITE

name: PE-18 (1)

statement

item
name: PE-18 (1)(a)

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

item
name: PE-18 (1)(b)

For existing facilities, consider the physical and environmental hazards in the organizational risk management strategy.

guidance

None.

INFORMATION LEAKAGE

name: PE-19

statement

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

guidance

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

NATIONAL EMISSIONS AND TEMPEST POLICIES AND PROCEDURES

name: PE-19 (1)

statement

Protect system components, associated data communications, and networks in accordance with national Emissions Security policies and procedures based on the security category or classification of the information.

guidance

Emissions Security (EMSEC) policies include the former TEMPEST policies.
None

References

FIPS Publication 199

ASSET MONITORING AND TRACKING

organization-defined asset location technologies
organization-defined asset location technologies

organization-defined assets
organization-defined assets

organization-defined controlled areas
organization-defined controlled areas

name: PE-20

statement

Employ to track and monitor the location and movement of within .

guidance

Asset location technologies can help organizations ensure that critical assets, including, for example, vehicles, equipment, or essential system components remain in authorized locations. Organizations consult with the Office of the General Counsel and the Senior Agency Official for Privacy regarding the deployment and use of asset location technologies to address potential privacy concerns.

ELECTROMAGNETIC PULSE PROTECTION

organization-defined security safeguards
organization-defined security safeguards

organization-defined systems and system components
organization-defined systems and system components
name: PE-21

statement

Employ against electromagnetic pulse damage for .

guidance

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

COMPONENT MARKING

organization-defined system hardware components
organization-defined system hardware components
name: PE-22

statement

Mark indicating the impact or classification level of the information permitted to be processed, stored, or transmitted by the hardware component.

guidance

Hardware components that may require marking include, for example, input devices marked to indicate the classification of the network to which they are connected or a multifunction function printer or copier residing in a classified area. Security marking refers to the application or use of human-readable security attributes. Security labeling refers to the application or

use of security attributes regarding internal data structures within systems. Security marking is generally not required for hardware components processing, storing, or transmitting information determined by organizations to be in the public domain or to be publicly releasable. However, organizations may require markings for hardware components processing, storing, or transmitting public information indicating that such information is publicly releasable. The marking of system hardware components reflects applicable laws, Executive Orders, directives, policies, regulations, standards, and guidelines.

PLANNING

PLANNING POLICY AND PROCEDURES

organization-defined personnel or roles
organization-defined personnel or roles

organization-defined senior management official
organization-defined senior management official

organization-defined frequency
organization-defined frequency

organization-defined frequency
organization-defined frequency
name: PL-1

statement

item
name: PL-1a.

Develop, document, and disseminate to :

item
name: PL-1a.1.

Security and privacy planning policies that:

item
name: PL-1a.1.(a)

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

item
name: PL-1a.1.(b)

Are consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and

item
name: PL-1a.2.

Procedures to facilitate the implementation of the security and privacy planning policies and the associated security and privacy planning controls;

item
name: PL-1b.

Designate an to manage the security and privacy planning policies and procedures;

item
name: PL-1c.

Review and update the current security and privacy planning:

item
name: PL-1c.1.

Policies ; and

item
name: PL-1c.2.

Procedures ;

item
name: PL-1d.

Ensure that the security and privacy planning procedures implement the security and privacy planning policies and controls; and

item
name: PL-1e.

Develop, document, and implement remediation actions for violations of the planning policy.

guidance

This control addresses the establishment of policy and procedures for the effective implementation of the controls and control enhancements in the PL family. The risk management strategy is an important factor in establishing policy and procedures. Comprehensive policy and procedures help provide security and privacy assurance. Security and privacy program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general security and privacy policies or can be represented by multiple policies reflecting the complex nature of

organizations. The procedures can be established for security and privacy programs and for systems, if needed. Procedures describe how policies or controls are implemented and can be directed at the personnel or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. It is important to recognize that restating controls does not constitute an organizational policy or procedure.

References

NIST Special Publication 800-12
NIST Special Publication 800-18
NIST Special Publication 800-30
NIST Special Publication 800-39
NIST Special Publication 800-100

SECURITY AND PRIVACY PLANS

organization-defined personnel or roles
organization-defined personnel or roles

organization-defined frequency
organization-defined frequency
name: PL-2

statement

item
name: PL-2a.

Develop security and privacy plans for the system that:

item
name: PL-2a.1.

Are consistent with the organization#s enterprise architecture;

item
name: PL-2a.2.

Explicitly define the authorization boundary for the system;

item
name: PL-2a.3.

Describe the operational context of the system in terms of missions and business processes;

item

name: PL-2a.4.

Provide the security categorization of the system including supporting rationale;

item
name: PL-2a.5.

Describe the operational environment for the system and relationships with or connections to other systems;

item
name: PL-2a.6.

Provide an overview of the security and privacy requirements for the system;

item
name: PL-2a.7.

Identify any relevant overlays, if applicable;

item
name: PL-2a.8.

Describe the security and privacy controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and

item
name: PL-2a.9.

Are reviewed and approved by the authorizing official or designated representative prior to plan implementation;

item
name: PL-2b.

Distribute copies of the security and privacy plans and communicate subsequent changes to the plans to ;

item
name: PL-2c.

Review the security and privacy plans ;

item
name: PL-2d.

Update the security and privacy plans to address changes to the system and environment of operation or problems identified during plan implementation or security and privacy control assessments; and

item

name: PL-2e.

Protect the security and privacy plans from unauthorized disclosure and modification.

guidance

Security and privacy plans relate security and privacy requirements to a set of security and privacy controls and control enhancements. The plans describe how the security and privacy controls and control enhancements meet those security and privacy requirements, but do not provide detailed, technical descriptions of the specific design or implementation of the controls and control enhancements. Security and privacy plans contain sufficient information (including the specification of parameter values for assignment and selection statements either explicitly or by reference) to enable a design and implementation that is unambiguously compliant with the intent of the plans and subsequent determinations of risk to organizational operations and assets, individuals, other organizations, and the Nation if the plan is implemented as intended. Organizations can also apply tailoring guidance to the control baselines in Appendix D to develop overlays for community-wide use or to address specialized requirements, technologies, missions, business applications, or environments of operation. Security and privacy plans need not be single documents. The plans can be a collection of various documents including documents that already exist. Effective security and privacy plans make extensive use of references to policies, procedures, and additional documents including, for example, design and implementation specifications where more detailed information can be obtained. This reduces the documentation associated with security and privacy programs and maintains the security- and privacy-related information in other established management and operational areas including, for example, enterprise architecture, system development life cycle, systems engineering, and acquisition. Thus, security and privacy plans do not contain detailed contingency plan or incident response plan information but instead provide explicitly or by reference, sufficient information to define what needs to be accomplished by those plans.

CONCEPT OF OPERATIONS

name: PL-2 (1)

statement

Incorporated into PL-7.

FUNCTIONAL ARCHITECTURE

name: PL-2 (2)

statement

Incorporated into PL-8.

PLAN AND COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES

organization-defined individuals or groups

organization-defined individuals or groups
name: PL-2 (3)

statement

Plan and coordinate security- and privacy-related activities affecting the system with before conducting such activities to reduce the impact on other organizational entities.

guidance

Security- and privacy-related activities include, for example, security and privacy assessments, audits and inspections, hardware and software maintenance, patch management, and contingency plan testing. Planning and coordination includes emergency and nonemergency (i.e., planned or non-urgent unplanned) situations. The process defined by organizations to plan and coordinate security- and privacy-related activities can be included in security and privacy plans for systems or other documents, as appropriate.

References
NIST Special Publication 800-18

SYSTEM SECURITY PLAN UPDATE
name: PL-3

statement

Incorporated into PL-2.

RULES OF BEHAVIOR

organization-defined frequency
organization-defined frequency

organization-defined frequency
organization-defined frequency
name: PL-4

statement

item
name: PL-4a.

Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy;

item

name: PL-4b.

Receive a documented acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system;

item
name: PL-4c.

Review and update the rules of behavior ; and

item
name: PL-4d.

Require individuals who have signed a previous version of the rules of behavior to read and re-sign [Selection (one or more): ; when the rules are revised or updated.]

guidance

This control enhancement applies to organizational users. Organizations consider rules of behavior based on individual user roles and responsibilities, differentiating, for example, between rules that apply to privileged users and rules that apply to the general user population. Establishing rules of behavior for some types of non-organizational users including, for example, individuals who simply receive data or information from federal systems, is often not feasible given the large number of such users and the limited nature of their interactions with the systems. Rules of behavior for organizational and non-organizational users can also be established in AC-8, System Use Notification. PL-4b, the documented acknowledgment portion of the control, may be satisfied by the security and privacy awareness training and the role-based security and privacy training programs conducted by organizations if such training includes rules of behavior. Documented acknowledgements for rules of behavior may include, for example, electronic or physical signatures; and electronic agreement check boxes/radio buttons.

SOCIAL MEDIA AND NETWORKING RESTRICTIONS

name: PL-4 (1)

statement

Include in the rules of behavior, explicit restrictions on the use of social media and networking sites and posting organizational information on public websites.

guidance

This control enhancement addresses rules of behavior related to the use of social media and networking sites when organizational personnel are using such sites for official duties or in the conduct of official business; when organizational information is involved in social media and networking transactions; and when personnel are accessing social media and networking sites from organizational systems. Organizations also address specific rules that prevent unauthorized entities from obtaining, either directly or through inference, non-public

organizational information from social media and networking sites. Examples of non-public information include system account information and personally identifiable information.
None

References
NIST Special Publication 800-18

PRIVACY IMPACT ASSESSMENT
name: PL-5

statement

Incorporated into RA-8.

SECURITY-RELATED ACTIVITY PLANNING
name: PL-6

statement

Incorporated into PL-2.

CONCEPT OF OPERATIONS

organization-defined frequency
organization-defined frequency
name: PL-7

statement

item
name: PL-7a.

Develop a Concept of Operations (CONOPS) for the system describing how the organization intends to operate the system from the perspective of information security and privacy; and

item
name: PL-7b.

Review and update the CONOPS .

guidance

The security and privacy CONOPS may be included in the security or privacy plans for the system or in other system development life cycle documents, as appropriate. Changes to the

CONOPS are reflected in ongoing updates to the security and privacy plans, the security and privacy architectures, and other appropriate organizational documents, including, for example, system development life cycle documents, procurement specifications, and systems engineering documents.

SECURITY AND PRIVACY ARCHITECTURES

organization-defined frequency
organization-defined frequency
name: PL-8

statement

item
name: PL-8a.

Develop security and privacy architectures for the system that:

item
name: PL-8a.1.

Describe the philosophy, requirements, and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information;

item
name: PL-8a.2.

Describe the philosophy, requirements, and approach to be taken for processing personally identifiable information;

item
name: PL-8a.3.

Describe how the security and privacy architectures are integrated into and support the enterprise architecture; and

item
name: PL-8a.4.

Describe any security- and privacy-related assumptions about, and dependencies on, external services;

item
name: PL-8b.

Review and update the security and privacy architectures to reflect updates in the enterprise architecture; and

item
name: PL-8c.

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

guidance

This control addresses actions taken by organizations in the design and development of systems. The security and privacy architectures at the system level are consistent with and complement the organization-wide security and privacy architectures described in PM-7 that are integral to and developed as part of the enterprise architecture. The security and privacy architectures include an architectural description, the placement and allocation of security and privacy functionality (including security and privacy controls), security- and privacy-related information for external interfaces, information being exchanged across the interfaces, and the protection mechanisms associated with each interface. In addition, the security and privacy architectures can include other information, for example, user roles and the access privileges assigned to each role, unique security and privacy requirements, types of information processed, stored, and transmitted by the system, restoration priorities of information and system services, and any other specific protection needs. In today#s modern computing architectures, it is becoming less common for organizations to control all information resources. There may be key dependencies on external information services and service providers. Describing such dependencies in the security and privacy architectures is important to developing a comprehensive mission and business protection strategy. Establishing, developing, documenting, and maintaining under configuration control, a baseline configuration for organizational systems is critical to implementing and maintaining effective security and privacy architectures. The development of the security and privacy architectures is coordinated with the Senior Agency Information Security Officer and the Senior Agency Official for Privacy to ensure that security and privacy controls needed to support security and privacy requirements are identified and effectively implemented. PL-8 is primarily directed at organizations to ensure that they develop security and privacy architectures for the system, and that the architectures are integrated with or tightly coupled to the enterprise architecture through the organization-wide security and privacy architectures. In contrast, SA-17 is primarily directed at external information technology product and system developers and integrators. SA-17, which is complementary to PL-8, is selected when organizations outsource the development of systems or system components to external entities, and there is a need to demonstrate consistency with the organization#s enterprise architecture and security and privacy architectures.

DEFENSE-IN-DEPTH

organization-defined security and privacy safeguards
organization-defined security and privacy safeguards

organization-defined locations and architectural layers
organization-defined locations and architectural layers

name: PL-8 (1)

statement

Design the security and privacy architectures for the system using a defense-in-depth approach that:

item
name: PL-8 (1)(a)

Allocates to ; and

item
name: PL-8 (1)(b)

Ensures that the allocated security and privacy safeguards operate in a coordinated and mutually reinforcing manner.

guidance

Organizations strategically allocate security safeguards (procedural, technical, or both) in the security architecture so that adversaries must overcome multiple safeguards to achieve their objective. Requiring adversaries to defeat multiple mechanisms makes it more difficult to successfully attack critical information resources by increasing the work factor of the adversary. It also increases the likelihood of detection. The coordination of allocated safeguards is essential to ensure that an attack that involves one safeguard does not create adverse unintended consequences by interfering with other safeguards. Examples of such unintended consequences include system lockout and cascading alarms. Placement of security safeguards is an important activity requiring thoughtful analysis. The criticality or value of the organizational asset is a key consideration in providing additional layering.

SUPPLIER DIVERSITY

organization-defined security and privacy safeguards
organization-defined security and privacy safeguards

organization-defined locations and architectural layers
organization-defined locations and architectural layers
name: PL-8 (2)

statement

Require that allocated to are obtained from different suppliers.

guidance

Different information technology products have different strengths and weaknesses. Providing a broad spectrum of products complements the individual offerings. For example, vendors offering

malicious code protection typically update their products at different times, often developing solutions for known viruses, Trojans, or worms based on their priorities and development schedules. By having different products at different locations there is an increased likelihood that at least one will detect the malicious code.

CENTRAL MANAGEMENT

organization-defined security and privacy controls and related processes
organization-defined security and privacy controls and related processes
name: PL-9

statement

Centrally manage .

guidance

Central management refers to the organization-wide management and implementation of selected security and privacy controls and related processes. This includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed controls and processes. As the central management of security and privacy controls is generally associated with the concept of common controls, such management promotes and facilitates standardization of control implementations and management and judicious use of organizational resources. Centrally-managed controls and processes may also meet independence requirements for assessments in support of initial and ongoing authorizations to operate and as part of organizational continuous monitoring. As part of the security and privacy control selection processes, organizations determine which controls may be suitable for central management based on organizational resources and capabilities. It is not always possible to centrally manage every aspect of a security or privacy control. In such cases, the control can be treated as a hybrid control with the control managed and implemented centrally or at the system level. Those controls and control enhancements that are candidates for full or partial central management include, but are not limited to: AC-2 (1) (2) (3) (4); AC-17 (1) (2) (3) (9); AC-18 (1) (3) (4) (5); AC-19 (4); AC-22; AC-23; AT-2 (1) (2); AT-3 (1) (2) (3); AT-4; AU-6 (1) (3) (5) (6) (9); AU-7 (1) (2); AU-11, AU-13, AU-16, CA-2 (1) (2) (3); CA-3 (1) (2) (3); CA-7 (1); CA-9; CM-2 (1) (2); CM-3 (1) (4); CM-4; CM-6 (1); CM-7 (4) (5); CM-8 (all); CM-9 (1); CM-10; CM-11; CP-7 (all); CP-8 (all); SC-43; SI-2; SI-3; SI-7; and SI-8.

References

NIST Special Publication 800-37

BASELINE SELECTION

name: PL-10

statement

Select a control baseline for the system.

guidance

The selection of an appropriate control baseline is determined by the needs of organizational stakeholders. Stakeholder needs and concerns consider mission and business requirements and mandates imposed by applicable laws, Executive Orders, directives, policies, regulations, standards, and guidelines. For example, the three control baselines in Appendix D are based on the requirements from the Federal Information Security Modernization Act (FISMA) and the Privacy Act. These requirements, along with the NIST standards and guidelines implementing the legislation, require organizations to select one of the control baselines after the reviewing the information types and the information that is processed, stored, and transmitted on organizational systems; analyzing the potential adverse impact or consequences of the loss or compromise of the system or information on the organization#s operations and assets, individuals, other organizations or the Nation; and considering the results from organizational and system assessments of risk. Nonfederal organizations that are part of other communities of interest including the U.S. critical infrastructure sectors, can develop similar control baselines (using the controls in Chapter Three) that represent the needs and concerns of those entities.

References

FIPS Publication 199
FIPS Publication 200
NIST Special Publication 800-30
NIST Special Publication 800-37
NIST Special Publication 800-39

BASELINE TAILORING

name: PL-11

statement

Tailor the selected control baseline by applying specified tailoring actions.

guidance

The concept of tailoring allows organizations to specialize or customize a set of baseline controls by applying a defined set of tailoring actions. These actions facilitate such specialization and customization by allowing organizations to develop security and privacy plans that reflect their specific missions and business functions, the environments where their systems operate, the threats and vulnerabilities that can affect their systems, and any other conditions or situations that can impact their mission or business success. The tailoring actions are described in Appendix G. Tailoring a control baseline is accomplished by identifying and designating

common controls; applying scoping considerations; selecting compensating controls; assigning values to control parameters; supplementing the control baseline with additional controls, as needed; and providing information for control implementation. The general tailoring actions in Appendix G can be supplemented with additional actions based on the needs of organizations. Tailoring actions can be applied to the baselines in Appendix D in accordance with the security requirements from the Federal Information Security Modernization Act (FISMA) and the privacy requirements from the Privacy Act. Alternatively, other communities of interest adopting different control baselines can apply the tailoring actions in Appendix G to specialize or customize the controls that represent the specific needs and concerns of those entities.

References

FIPS Publication 199
FIPS Publication 200
NIST Special Publication 800-30
NIST Special Publication 800-37
NIST Special Publication 800-39

PROGRAM MANAGEMENT

INFORMATION SECURITY PROGRAM PLAN

organization-defined frequency
organization-defined frequency
name: PM-1

statement

item
name: PM-1a.

Develop and disseminate an organization-wide information security program plan that:

item
name: PM-1a.1.

Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;

item
name: PM-1a.2.

Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance;

item
name: PM-1a.3.

Reflects the coordination among organizational entities responsible for information security; and

item
name: PM-1a.4.

Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation;

item
name: PM-1b.

Review the organization-wide information security program plan ;

item
name: PM-1c.

Update the information security program plan to address organizational changes and problems identified during plan implementation or control assessments; and

item
name: PM-1d.

Protect the information security program plan from unauthorized disclosure and modification.

guidance

Information security program plans can be represented in single documents or compilations of documents at the discretion of organizations. The plans document the program management controls and organization-defined common controls. Information security program plans provide sufficient information about the program management controls/common controls (including specification of parameters for any assignment and selection statements either explicitly or by reference) to enable implementations that are unambiguously compliant with the intent of the plans and a determination of the risk to be incurred if the plans are implemented as intended. Security plans for individual systems and the organization-wide information security program plan, provide complete coverage for all security controls employed within the organization. Common controls are documented in an appendix to the organization#s information security program plan unless the controls are included in a separate security plan for a system. The organization-wide information security program plan will indicate which separate security plans contain descriptions of common controls. Organizations have the flexibility to describe common controls in a single document or in multiple documents. For multiple documents, the documents describing common controls are included as attachments to the information security program plan. If the information security program plan contains multiple documents, the organization specifies in each document the organizational official or officials responsible for

the development, implementation, assessment, authorization, and monitoring of the respective common controls. For example, the Facilities Management Office may develop, implement, assess, authorize, and continuously monitor common physical and environmental protection controls from the PE family when such controls are not associated with a particular system but instead, support multiple systems.

INFORMATION SECURITY PROGRAM ROLES

name: PM-2

statement

item
name: PM-2a.

Appoint a Senior Agency Information Security Officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program;

item
name: PM-2b.

Appoint a Senior Accountable Official for Risk Management to align information security management proceeses with strategic, operational, and budgetary planning procceses; and

item
name: PM-2c.

Appoint a Risk Executive (function) to view and analyze risk from an organization-wide perspective and ensure management of risk is consistent across the organization.

guidance

The senior information security officer is an organizational official. For federal agencies (as defined by applicable laws, Executive Orders, regulations, directives, policies, and standards), this official is the Senior Agency Information Security Officer. Organizations may also refer to this official as the Senior Information Security Officer or Chief Information Security Officer. The senior accountable official for risk management leads the risk executive (function) in organization-wide risk management activities.
None

References
NIST Special Publication 800-37
NIST Special Publication 800-39

INFORMATION SECURITY AND PRIVACY RESOURCES

name: PM-3

statement

item
name: PM-3a.

Include the resources needed to implement the information security and privacy programs in capital planning and investment requests and document all exceptions to this requirement;

item
name: PM-3b.

Prepare documentation required for addressing information security and privacy programs in capital planning and investment requests in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards; and

item
name: PM-3c.

Make available for expenditure, the planned information security and privacy resources.

guidance

Organizations consider establishing champions for information security and privacy efforts and as part of including the necessary resources, assign specialized expertise and resources as needed. Organizations may designate and empower an Investment Review Board or similar group to manage and provide oversight for the information security-and privacy-related aspects of the capital planning and investment control process.

References

NIST Special Publication 800-65

PLAN OF ACTION AND MILESTONES PROCESS

name: PM-4

statement

item
name: PM-4a.

Implement a process to ensure that plans of action and milestones for the security and privacy programs and associated organizational systems:

item
name: PM-4a.1.

Are developed and maintained;

item
name: PM-4a.2.

Document the remedial information security and privacy actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and

item
name: PM-4a.3.

Are reported in accordance with established reporting requirements.

item
name: PM-4b.

Review plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

guidance

The plan of action and milestones is a key document in the information security and privacy programs and is subject to reporting requirements established by the Office of Management and Budget. Organizations view plans of action and milestones from an enterprise-wide perspective, prioritizing risk response actions and ensuring consistency with the goals and objectives of the organization. Plan of action and milestones updates are based on findings from control assessments and continuous monitoring activities.
CA-5; CA-7

References
NIST Special Publication 800-37

SYSTEM INVENTORY
name: PM-5

statement

Develop and maintain an inventory of organizational systems.

guidance

OMB provides guidance on developing systems inventories and associated reporting requirements. This control refers to an organization-wide inventory of systems, not system components as described in CM-8.

None

MEASURES OF PERFORMANCE

name: PM-6

statement

Develop, monitor, and report on the results of information security and privacy measures of performance.

guidance

Measures of performance are outcome-based metrics used by an organization to measure the effectiveness or efficiency of the information security and privacy programs and the security and privacy controls employed in support of the program.

References

NIST Special Publication 800-55
NIST Special Publication 800-137

ENTERPRISE ARCHITECTURE

name: PM-7

statement

Develop an enterprise architecture with consideration for information security, privacy, and the resulting risk to organizational operations and assets, individuals, other organizations, and the Nation.

guidance

The integration of security and privacy requirements and controls into the enterprise architecture ensures that security and privacy considerations are addressed early in the system development life cycle and are directly and explicitly related to the organization#s mission and business processes. The process of security and privacy requirements integration also embeds into the enterprise architecture, the organization#s security and privacy architectures consistent with the organizational risk management and information security and privacy strategies. For PM-7, the security and privacy architectures are developed at a system-of-systems level, representing all organizational systems. For PL-8, the security and privacy architectures are developed at a level representing an individual system. The system-level architectures are consistent with the security and privacy architectures defined for the organization. Security and privacy requirements and control integration are most effectively accomplished through the rigorous application of the Risk Management Framework and supporting security standards and guidelines.

References
NIST Special Publication 800-39

CRITICAL INFRASTRUCTURE PLAN

name: PM-8

statement

Address information security and privacy issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

guidance

Protection strategies are based on the prioritization of critical assets and resources. The requirement and guidance for defining critical infrastructure and key resources and for preparing an associated critical infrastructure protection plan are found in applicable laws, Executive Orders, directives, policies, regulations, standards, and guidelines.

References
HSPD 7
National Infrastructure Protection Plan

RISK MANAGEMENT STRATEGY

organization-defined frequency
organization-defined frequency
name: PM-9

statement

item
name: PM-9a.

Develops a comprehensive strategy to manage:

item
name: PM-9a.1.

Security risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of organizational systems;

item
name: PM-9a.2.

Privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of personally identifiable information; and

item
name: PM-9a.3.

Supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services;

item
name: PM-9b.

Implement the risk management strategy consistently across the organization; and

item
name: PM-9c.

Review and update the risk management strategy or as required, to address organizational changes.

guidance

An organization-wide risk management strategy includes, for example, an expression of the security, privacy, and supply chain risk tolerance for the organization; acceptable risk assessment methodologies; security, privacy, and supply chain risk mitigation strategies; a process for consistently evaluating security, privacy, and supply chain risk across the organization with respect to the organization#s risk tolerance; and approaches for monitoring risk over time. The senior accountable official for risk management (agency head or designated official) aligns information security management proceeses with strategic, operational, and budgetary planning procceses. The use of a risk executive function, led by the senior accountable official for risk management, can facilitate consistent application of the risk management strategy organization-wide. The organization-wide risk management strategy can be informed by security, privacy, and supply chain risk-related inputs from other sources, internal and external to the organization, to ensure the strategy is both broad-based and comprehensive.
All XX-1 Controls

References

NIST Special Publication 800-30
NIST Special Publication 800-39
NIST Special Publication 800-161

AUTHORIZATION PROCESS

name: PM-10

statement

item
name: PM-10a.

Manage the security and privacy state of organizational systems and the environments in which those systems operate through authorization processes;

item
name: PM-10b.

Designate individuals to fulfill specific roles and responsibilities within the organizational risk management process; and

item
name: PM-10c.

Integrate the authorization processes into an organization-wide risk management program.

guidance

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

References
NIST Special Publication 800-37
NIST Special Publication 800-39

MISSION AND BUSINESS PROCESS DEFINITION

organization-defined frequency
organization-defined frequency
name: PM-11

statement

item
name: PM-11a.

Define organizational mission and business processes with consideration for information security and privacy and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and

item
name: PM-11b.

Determine information protection and personally identifiable information processing needs arising from the defined mission and business processes; and

item
name: PM-11c.

Review and revise the mission and business processes , until achievable protection and personally identifiable information processing needs are obtained.

guidance

Protection needs are technology-independent, required capabilities to counter threats to organizations, individuals, systems, and the Nation through the compromise of information (i.e., loss of confidentiality, integrity, availability, or privacy). Information protection and personally identifiable information processing needs are derived from mission and business needs defined by the stakeholders in organizations, the mission and business processes defined to meet those needs, and the organizational risk management strategy. Information protection and personally identifiable information processing needs determine the required security and privacy controls for the organization and the systems supporting the mission and business processes. Inherent in defining the protection and personally identifiable information processing needs, is an understanding of adverse impact or consequences that could result if a compromise of information occurs. The categorization process is used to make such potential impact determinations. Privacy risks to individuals can arise from the compromise of personally identifiable information, but they can also arise as unintended consequences or a byproduct of authorized processing of information at any stage of the data life cycle. Privacy risk assessments are used to prioritize the risks that are created for individuals from system processing of personally identifiable information. These risk assessments enable the selection of the required privacy controls for the organization and systems supporting the mission and business processes. Mission and business process definitions and the associated protection requirements are documented in accordance with organizational policy and procedures.

References
FIPS Publication 199

INSIDER THREAT PROGRAM
name: PM-12

statement

Implement an insider threat program that includes a cross-discipline insider threat incident handling team.

guidance

Organizations handling classified information are required, under Executive Order 13587 and the National Policy on Insider Threat, to establish insider threat programs. The standards and guidelines that apply to insider threat programs in classified environments can also be employed effectively to improve the security of Controlled Unclassified Information in non-national security systems. Insider threat programs include controls to detect and prevent malicious insider activity through the centralized integration and analysis of both technical and non-technical information to identify potential insider threat concerns. A senior official is designated by the department or agency head as the responsible individual to implement and provide oversight for the program. In addition to the centralized integration and analysis capability, insider threat programs as a minimum, prepare department or agency insider threat policies and implementation plans; conduct host-based user monitoring of individual employee activities on government-owned classified computers; provide insider threat awareness training to employees; receive access to information from all offices within the department or agency for insider threat analysis; and conduct self-assessments of department or agency insider threat posture. Insider threat programs can leverage the existence of incident handling teams that organizations may already have in place, such as computer security incident response teams. Human resources records are especially important in this effort, as there is compelling evidence to show that some types of insider crimes are often preceded by nontechnical behaviors in the workplace including, for example, ongoing patterns of disgruntled behavior and conflicts with coworkers and other colleagues. These precursors can better inform and guide organizational officials in more focused, targeted monitoring efforts. However, the use of human resource records could raise significant concerns for privacy. The participation of a comprehensive legal team, including consultation with the senior agency officer for privacy (SAOP), ensures that all monitoring activities are performed in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines.

SECURITY AND PRIVACY WORKFORCE

name: PM-13

statement

Establish a security and privacy workforce development and improvement program.

guidance

Security and privacy workforce development and improvement programs include, for example, defining the knowledge, skills, and abilities needed to perform security and privacy duties and tasks; developing role-based training programs for individuals assigned security and privacy roles and responsibilities; and providing standards and guidelines for measuring and building individual qualifications for incumbents and applicants for security- and privacy-related positions. Such workforce development and improvement programs can also include

security and privacy career paths to encourage security and privacy professionals to advance in the field and fill positions with greater responsibility. The programs encourage organizations to fill security- and privacy-related positions with qualified personnel. Security and privacy workforce development and improvement programs are complementary to organizational security awareness and training programs and focus on developing and institutionalizing the core security and privacy capabilities of personnel needed to protect organizational operations, assets, and individuals.

TESTING, TRAINING, AND MONITORING

name: PM-14

statement

item

name: PM-14a.

Implement a process for ensuring that organizational plans for conducting security and privacy testing, training, and monitoring activities associated with organizational systems:

item

name: PM-14a.1.

Are developed and maintained; and

item

name: PM-14a.2.

Continue to be executed in a timely manner;

item

name: PM-14b.

Review testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

guidance

This control ensures that organizations provide oversight for the security and privacy testing, training, and monitoring activities conducted organization-wide and that those activities are coordinated. With the growing importance of continuous monitoring programs, the implementation of information security and privacy across the three tiers of the risk management hierarchy and the widespread use of common controls, organizations coordinate and consolidate the testing and monitoring activities that are routinely conducted as part of ongoing organizational assessments supporting a variety of security and privacy controls. Security and privacy training activities, while focused on individual systems and specific

roles, also necessitate coordination across all organizational elements. Testing, training, and monitoring plans and activities are informed by current threat and vulnerability assessments.

References

NIST Special Publication 800-37
NIST Special Publication 800-39

CONTACTS WITH GROUPS AND ASSOCIATIONS

name: PM-15

statement

Establish and institutionalize contact with selected groups and associations within the security and privacy communities:

item
name: PM-15a.

To facilitate ongoing security and privacy education and training for organizational personnel;

item
name: PM-15b.

To maintain currency with recommended security and privacy practices, techniques, and technologies; and

item
name: PM-15c.

To share current security- and privacy-related information including threats, vulnerabilities, and incidents.

guidance

Ongoing contact with security and privacy groups and associations is of paramount importance in an environment of rapidly changing technologies and threats. Security and privacy groups and associations include, for example, special interest groups, professional associations, forums, news groups, and peer groups of security and privacy professionals in similar organizations. Organizations select groups and associations based on organizational missions and business functions. Organizations share threat, vulnerability, privacy problems, contextual insights, compliance techniques, and incident information consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidelines.

THREAT AWARENESS PROGRAM

name: PM-16

statement

Implement a threat awareness program that includes a cross-organization information-sharing capability.

guidance

Because of the constantly changing and increasing sophistication of adversaries, especially the advanced persistent threat (APT), it may be more likely that adversaries can successfully breach or compromise organizational systems. One of the best techniques to address this concern is for organizations to share threat information. This can include sharing threat events (i.e., tactics, techniques, and procedures) that organizations have experienced, mitigations that organizations have found are effective against certain types of threats, and threat intelligence (i.e., indications and warnings about threats that can occur). Threat information sharing may be bilateral or multilateral. Examples of bilateral threat sharing include government-commercial cooperatives and government-government cooperatives. An example of multilateral sharing includes organizations taking part in threat-sharing consortia. Threat information may be highly sensitive requiring special agreements and protection, or less sensitive and freely shared.

AUTOMATED MEANS FOR SHARING THREAT INTELLIGENCE

name: PM-16 (1)

statement

Utilize automated means to maximize the effectiveness of sharing threat intelligence information.

guidance

To maximize the effectiveness of monitoring, it is important to know what threat observables and indicators the sensors need to be searching for. By utilizing well established frameworks, services, and automated tools, organizations greatly improve their ability to rapidly share and feed into monitoring tools, the relevant threat detection signatures.
None

PROTECTING CONTROLLED UNCLASSIFIED INFORMATION ON EXTERNAL SYSTEMS

organization-defined frequency
organization-defined frequency

name: PM-17

statement

item
name: PM-17a.

Establish policy and procedures to ensure that the requirements for the protection of Controlled Unclassified Information processed, stored or transmitted on external systems, are implemented in accordance with applicable laws, Executive Orders, directives, policies, regulations, and standards.

item
name: PM-17b.

Update the policy and procedures .

guidance

The protection of Controlled Unclassified Information (CUI) in nonfederal organizations and systems is critical to the security of federal operations and assets and the privacy of individuals. CUI is defined by the National Archives and Records Administration along with the appropriate safeguarding and dissemination requirements for such information and is codified in 32 CFR 2002, Controlled Unclassified Information and specifically, for systems external to the federal organization, in 32 CFR 2002.14h. The policy prescribes the specific use and conditions to be implemented in accordance with organizational procedures including, for example, via its contracting processes.

PRIVACY PROGRAM PLAN
name: PM-18

statement

item
name: PM-18a.

Develop and disseminate an organization-wide privacy program plan that provides an overview of the agency#s privacy program, and:

item
name: PM-18a.1.

Includes a description of the structure of the privacy program and the resources dedicated to the privacy program;

item
name: PM-18a.2.

Provides an overview of the requirements for the privacy program and a description of the privacy program management controls and common controls in place or planned for meeting those requirements;

item
name: PM-18a.3.

Includes the role of the Senior Agency Official for Privacy and the identification and assignment of roles of other privacy officials and staff and their responsibilities;

item
name: PM-18a.4.

Describes management commitment, compliance, and the strategic goals and objectives of the privacy program;

item
name: PM-18a.5.

Reflects coordination among organizational entities responsible for the different aspects of privacy; and

item
name: PM-18a.6.

Is approved by a senior official with responsibility and accountability for the privacy risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; and

item
name: PM-18b.

Update the plan to address changes in federal privacy laws and policy and organizational changes and problems identified during plan implementation or privacy control assessments.

guidance

A Privacy program plan is a formal document that provides an overview of an organization#s privacy program, including a description of the structure of the privacy program, the resources dedicated to the privacy program, the role of the Senior Agency Official for Privacy and other privacy officials and staff, the strategic goals and objectives of the privacy program, and the program management and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks. Privacy program plans can be integrated with information security plans or can be represented independently, either in a single document or in compilations of documents at the discretion of organizations. The plans document the program management controls and organization-defined common controls. Privacy program plans provide sufficient information about the program management and common controls (including specification of parameters and assignment and selection statements either explicitly or by

reference) to enable control implementations that are unambiguously compliant with the intent of the plans and a determination of the risk incurred if the plans are implemented as intended. The privacy plans for individual systems and the organization-wide privacy program plan together provide complete coverage for all privacy controls employed within the organization. Common controls are documented in an appendix to the organization#s privacy program plan unless the controls are included in a separate privacy plan for a system. The organization-wide privacy program plan indicates which separate privacy plans contain descriptions of privacy controls. Organizations have the flexibility to describe common controls in a single document or in multiple documents. In the case of multiple documents, the documents describing common controls are included as attachments to the privacy program plan. If the privacy program plan contains multiple documents, the organization specifies in each document, the organizational official or officials responsible for the development, implementation, assessment, authorization, and monitoring of the respective common controls.

PRIVACY PROGRAM ROLES

name: PM-19

statement

Appoint a Senior Agency Official for Privacy with the authority, mission, accountability, and resources to coordinate, develop, and implement, applicable privacy requirements and manage privacy risks through the organization-wide privacy program.

guidance

The privacy officer described in this control is an organizational official. For federal agencies, as defined by applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines, this official is designated as the Senior Agency Official for Privacy. Organizations may also refer to this official as the Chief Privacy Officer.

SYSTEM OF RECORDS NOTICE

name: PM-20

statement

item

name: PM-20a.

Publish System of Records Notices in the Federal Register, subject to required oversight processes, for systems containing personally identifiable information; and

item

name: PM-20b.

Keep System of Records Notices current.

guidance

Organizations issue System of Records Notices to provide the public notice regarding personally identifiable information collected in a system of records. The Privacy Act defines a system of records as a group of any records under the control of any agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifier. System of Records Notices explain how the information is used, retained, and may be corrected, and whether certain portions of the system are subject to Privacy Act exemptions for law enforcement or national security reasons.

DISSEMINATION OF PRIVACY PROGRAM INFORMATION

name: PM-21

statement

item
name: PM-21a.

Ensure that the public has access to information about organizational privacy activities and can communicate with its Senior Agency Official for Privacy;

item
name: PM-21b.

Ensure that organizational privacy practices are publicly available through organizational websites or otherwise; and

item
name: PM-21c.

Employ publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to privacy offices regarding privacy practices.

guidance

Organizations employ different mechanisms for informing the public about their privacy practices including, for example, Privacy Impact Assessments, System of Records Notices, privacy reports, publicly available web pages, email distributions, blogs, and periodic publications, including, for example, quarterly newsletters.

ACCOUNTING OF DISCLOSURES

name: PM-22

statement

item
name: PM-22a.

Develop and maintain an accounting of disclosures of personally identifiable information held in each system of records under its control, including:

item
name: PM-22a.1.

Date, nature, and purpose of each disclosure of a record; and

item
name: PM-22a.2.

Name and address of the person or organization to which the disclosure was made;

item
name: PM-22b.

Retain the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer; and

item
name: PM-22c.

Make the accounting of disclosures available to the person named in the record upon request.

guidance

This control addresses disclosure accounting requirements in the Privacy Act. The purpose of disclosure accounting requirements is to allow individuals to learn to whom records about them have been disclosed; to provide a basis for subsequently advising recipients of records of any corrected or disputed records; and to provide an audit trail for subsequent reviews of organizational compliance with conditions for disclosures. Organizations can use any system for keeping notations of disclosures, if it can construct from such a system, a document listing of all disclosures. Automated mechanisms can be used by organizations to determine when such information is disclosed, including, for example, commercial services providing notifications and alerts. Accounting of disclosures may also be used to help organizations verify compliance with applicable privacy statutes and policies governing disclosure or dissemination of information and dissemination restrictions.

DATA QUALITY MANAGEMENT
name: PM-23

statement

Issue guidelines ensuring and maximizing the quality, utility, objectivity, integrity, impact determination, and de-identification of personally identifiable information across the information life cycle.

guidance

Data quality management guidelines include the reasonable steps that organizations take to confirm the accuracy and relevance of personally identifiable information throughout the information life cycle. The information life cycle includes the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposition of personally identifiable information. Such steps may include, for example, editing and validating addresses as they are collected or entered into systems using automated address verification look-up application programming interfaces. The measures taken to protect data quality are based on the nature and context of the personally identifiable information, how it is to be used, how it was obtained, the impact level of the personally identifiable information obtained, and potential de-identification methods employed. Measures taken to validate the accuracy of personally identifiable information that is used to make determinations about the rights, benefits, or privileges of individuals under federal programs may be more comprehensive than those used to validate less sensitive personally identifiable information. Additional steps may be necessary to validate personally identifiable information that is obtained from sources other than individuals or the authorized representatives of individuals.

AUTOMATION

name: PM-23 (1)

statement

Issue technical guidelines and documentation to support automated evaluation of data quality across the information life cycle.

guidance

As data is obtained and used across the information life cycle, it is important to confirm the accuracy and relevance of personally identifiable information. Automated tools and techniques can augment existing process and procedures and enable an organization to better identify and manage personally identifiable information in large-scale systems. For example, automated tools can greatly improve efforts to consistently normalize data or identify malformed data. Automated tools can also be used to improve auditing of data, to track how data is used across the information life cycle, and to detect errors that may incorrectly alter personally identifiable information or incorrectly associate such information with the wrong individual. These automated capabilities backstop processes and procedures at-scale. They also enable more fine-grained detection and correction of data quality errors.

None

DATA TAGGING

name: PM-23 (2)

statement

Issue data modeling guidelines to support tagging of personally identifiable information.

guidance

Data tagging includes, for example, tags noting the authority to collect, usage, presence of personally identifiable information, de-identification, impact level, and information life cycle stage.

UPDATING PERSONALLY IDENTIFIABLE INFORMATION

name: PM-23 (3)

statement

When managing personally identifiable information, develop procedures and incorporate mechanisms to identify and record the method under which the information is updated, and the frequency that such updates occur.

guidance

When managing personally identifiable information including, for example, health information and financial information, it is important to carefully track updates or changes to such data. Having the ability to track both the method and frequency of updates enhances transparency and individual participation. It also enables individuals to better understand how and when their information is changed and helps both individuals and the responsible organizations to know how and what personally identifiable information was changed should erroneous information be identified.
None

DATA MANAGEMENT BOARD

organization-defined roles
organization-defined roles
name: PM-24

statement

item
name: PM-24a.

Establish a written charter for a Data Management Board;

item
name: PM-24b.

Establish the Data Management Board consisting of with the following responsibilities:

item
name: PM-24b.1.

Develop and implement guidelines supporting data modeling, quality, integrity, and de-identification needs of personally identifiable information across the information life cycle;

item
name: PM-24b.2.

Review and approve applications to release data outside of the organization, archiving the applications and the released data, and performing post-release monitoring to ensure that the assumptions made as part of the data release continue to be valid;

item
name: PM-24c.

Include requirements for personnel interaction with the Data Management Board in security and privacy awareness and/or role-based training.

guidance

The guidelines established by Data Management Board establish policies, procedures, and standards that enable data governance so that personally identifiable information is managed and maintained in accordance with any relevant statutes, regulations, and guidance. Members may include the Chief Information Officer, Senior Agency Information Security Officer, and Senior Agency Official for Privacy. With respect to data modeling, and the quality, integrity, and de-identification of personally identifiable information, data and information needs are met through organization-wide data governance policies that establish the roles, responsibilities, and processes by which personnel manage information as an asset across the information life cycle. The information life cycle includes creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposition. Members may include the Chief Information Officer, Senior Agency Official for Privacy, and Senior Agency Information Security Officer.

DATA INTEGRITY BOARD

name: PM-25

statement

Establish a Data Integrity Board to oversee organizational Computer Matching Agreements.

guidance

Organizations executing Computer Matching Agreements or participating in such agreements with other organizations regarding applicants for and recipients of financial assistance or payments under federal benefit programs or certain computerized comparisons involving federal personnel or payroll records, establish a Data Integrity Board to oversee and coordinate

the implementation of those matching agreements. As data is obtained and used across the information life cycle, it is important to confirm the accuracy and relevance of personally identifiable information. Organizations may integrate the function of the Data Integrity Board into the responsibilities of the Data Management Board under PM-24. In many organizations, the Data Integrity Board is led by the Senior Agency Official for Privacy.

PUBLISH AGREEMENTS ON WEBSITE

name: PM-25 (1)

statement

Publish Computer Matching Agreements on the public website of the organization.

guidance

None.
None

MINIMIZATION OF PERSONALLY IDENTIFIABLE INFORMATION USED IN TESTING, TRAINING, AND RESEARCH

name: PM-26

statement

item

name: PM-26a.

Develop and implement policies and procedures that address the use of personally identifiable information for internal testing, training, and research;

item

name: PM-26b.

Take measures to limit or minimize the amount of personally identifiable information used for internal testing, training, and research purposes; and

item

name: PM-26c.

Authorize the use of personally identifiable information when such information is required for internal testing, training, and research.

guidance

Organizations often use personally identifiable information for testing new applications or systems prior to deployment, for research purposes, and for training. The use of personally identifiable information in testing, research, and training increases risk of unauthorized

disclosure or misuse of such information. Organizations consult with the Senior Agency Official for Privacy and legal counsel to ensure that the use of personally identifiable information in testing, training, and research is compatible with the original purpose for which it was collected. When possible, organizations use placeholder data to avoid exposure of personally identifiable information when conducting testing, training, and research.

INDIVIDUAL ACCESS CONTROL

name: PM-27

statement

item

name: PM-27a.

Publish:

item

name: PM-27a.1.

Policies governing how individuals may request access to records maintained in a Privacy Act system of records; and

item

name: PM-27a.2.

Access procedures in System of Records Notices; and

item

name: PM-27b.

Ensure that the published policies and access procedures are consistent with Privacy Act requirements and Office of Management and Budget policies and guidance for the proper processing of Privacy Act requests.

guidance

Access affords individuals the ability to review personally identifiable information about them held within organizational systems of records. Access includes timely, simplified, and inexpensive access to data. Organizational processes for allowing access to records may differ based on resources, legal requirements, or other factors. The Senior Agency Official for Privacy is responsible for the content of Privacy Act regulations and record request processing, in consultation with the organization#s legal counsel. Access to certain types of records may not be appropriate, however, and heads of agencies may promulgate rules exempting particular systems from the access provision of the Privacy Act.

COMPLAINT MANAGEMENT

name: PM-28

statement

Implement a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices that includes:

item
name: PM-28a.

Mechanisms that are easy to use and readily accessible by the public;

item
name: PM-28b.

All information necessary for successfully filing complaints; and

item
name: PM-28c.

Tracking mechanisms to ensure all complaints received are reviewed and appropriately addressed in a timely manner.

guidance

Complaints, concerns, and questions from individuals can serve as a valuable source of external input that ultimately improves operational models, uses of technology, data collection practices, and privacy and security controls. Mechanisms that can be used by the public may include, for example, e-mail, telephone hotline, or web-based forms. Information necessary for successfully filing complaints includes, for example, contact information for the Senior Agency Official for Privacy or other official designated to receive complaints.

INVENTORY OF PERSONALLY IDENTIFIABLE INFORMATION

organization-defined frequency
organization-defined frequency

organization-defined frequency
organization-defined frequency

organization-defined frequency
organization-defined frequency
name: PM-29

statement

item
name: PM-29a.

Establish, maintain, and update an inventory of all programs and systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of personally identifiable information;

item
name: PM-29b.

Provide updates of the personally identifiable information inventory to the Chief Information Officer, Senior Agency Official for Privacy, and Senior Agency Information Security Officer ;

item
name: PM-29c.

Use the personally identifiable information inventory to support the establishment of information security and privacy requirements for all new or modified systems containing personally identifiable information;

item
name: PM-29d.

Review the personally identifiable information inventory ;

item
name: PM-29e.

Ensure to the extent practicable, that personally identifiable information is accurate, relevant, timely, and complete; and

item
name: PM-29f.

Reduce personally identifiable information to the minimum necessary for the proper performance of authorized organizational functions.

guidance

Organizations coordinate with federal records officers to ensure that reductions in organizational holdings of personally identifiable information are consistent with National Archives and Records Administration retention schedules. By performing periodic assessments, organizations ensure that only the data specified in the notice is collected, and that the data collected is still relevant and necessary for the purpose specified in privacy notices. The set of personally identifiable information elements required to support an organizational mission or business process may be a subset of the personally identifiable information the organization is authorized to collect.

AUTOMATION SUPPORT

name: PM-29 (1)

statement

Employ automated mechanisms to determine if personally identifiable information is maintained in electronic form.

guidance

Automated mechanisms include, for example, commercial services providing notifications and alerts to organizations about where personally identifiable information is stored.
None

PRIVACY REPORTING

organization-defined officials
organization-defined officials
name: PM-30

statement

Develop, disseminate, and update privacy reports to:

item
name: PM-30a.

The Office of Management and Budget, Congress, and other oversight bodies to demonstrate accountability with statutory and regulatory privacy program mandates; and

item
name: PM-30b.

and other personnel with responsibility for monitoring privacy program progress and compliance.

guidance

Through internal and external privacy reporting, organizations promote accountability and transparency in organizational privacy operations. Reporting can also help organizations to determine progress in meeting privacy compliance requirements and privacy controls, compare performance across the federal government, identify vulnerabilities and gaps in policy and implementation, and identify success models. Privacy reports include, for example, annual Senior Agency Official for Privacy reports to OMB; reports to Congress required by the Implementing Regulations of the 9/11 Commission Act; and other public reports required by specific statutory mandates or internal policies of organizations. The Senior Agency Official for Privacy consults with legal counsel, where appropriate, to ensure that organizations meet all applicable privacy reporting requirements.

SUPPLY CHAIN RISK MANAGEMENT PLAN

organization-defined frequency
organization-defined frequency
name: PM-31

statement

item
name: PM-31a.

Develop a plan for managing supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services;

item
name: PM-31b.

Implement the supply chain risk management plan consistently across the organization; and

item
name: PM-31c.

Review and update the supply chain risk management plan or as required, to address organizational changes.

guidance

An organization-wide supply chain risk management plan includes, for example, an unambiguous expression of the supply chain risk tolerance for the organization, acceptable supply chain risk mitigation strategies or controls, a process for consistently evaluating and monitoring supply chain risk, approaches for implementing and communicating the supply chain risk management plan, and associated roles and responsibilities. The organization-wide supply chain risk management plan can be incorporated into the organization#s risk management strategy and be used to inform the system-level supply chain risk management plan. The use of a risk executive function can facilitate consistent, organization-wide application of the supply chain risk management plan.

References
NIST Special Publication 800-161

RISK FRAMING
name: PM-32

statement

item
name: PM-32a.

Identify assumptions affecting risk assessments, risk response, and risk monitoring;

item
name: PM-32b.

Identify constraints affecting risk assessments, risk response, and risk monitoring;

item
name: PM-32c.

Identify the organizational risk tolerance; and

item
name: PM-32d.

Identify priorities and trade-offs considered by the organization for managing risk.

guidance

Risk framing is most effectively conducted at the organization-wide level. The assumptions, constraints, organizational risk tolerance, and priorities and trade-offs identified for this control inform the organizational risk management strategy which in turn, informs the conduct of risk assessment, risk response, and risk monitoring.

References
NIST Special Publication 800-39

PERSONNEL SECURITY

PERSONNEL SECURITY POLICY AND PROCEDURES

organization-defined personnel or roles
organization-defined personnel or roles

organization-defined senior management official
organization-defined senior management official

organization-defined frequency
organization-defined frequency

organization-defined frequency
organization-defined frequency
name: PS-1

statement

item
name: PS-1a.

Develop, document, and disseminate to :

item
name: PS-1a.1.

A personnel security policy that:

item
name: PS-1a.1.(a)

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

item
name: PS-1a.1.(b)

Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and

item
name: PS-1a.2.

Procedures to facilitate the implementation of the personnel security policy and the associated personnel security controls;

item
name: PS-1b.

Designate an to manage the personnel security policy and procedures;

item
name: PS-1c.

Review and update the current personnel security:

item
name: PS-1c.1.

Policy ; and

item
name: PS-1c.2.

Procedures ;

item
name: PS-1d.

Ensure that the personnel security procedures implement the personnel security policy and controls; and

item
name: PS-1e.

Develop, document, and implement remediation actions for violations of the personnel security policy.

guidance

This control addresses the establishment of policy and procedures for the effective implementation of the controls and control enhancements in the PS family. The risk management strategy is an important factor in establishing policy and procedures. Comprehensive policy and procedures help provide security and privacy assurance. Security and privacy program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general security and privacy policy or can be represented by multiple policies reflecting the complex nature of organizations. The procedures can be established for security and privacy programs and for systems, if needed. Procedures describe how policies or controls are implemented and can be directed at the personnel or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. It is important to recognize that restating controls does not constitute an organizational policy or procedure.

References

NIST Special Publication 800-12
NIST Special Publication 800-30
NIST Special Publication 800-39
NIST Special Publication 800-100

POSITION RISK DESIGNATION

organization-defined frequency
organization-defined frequency
name: PS-2

statement

item
name: PS-2a.

Assign a risk designation to all organizational positions;

item

name: PS-2b.

Establish screening criteria for individuals filling those positions; and

item
name: PS-2c.

Review and update position risk designations .

guidance

Position risk designations reflect Office of Personnel Management policy and guidance. Risk designations can guide and inform the types of authorizations individuals receive when accessing organizational information and systems. Position screening criteria include explicit information security role appointment requirements.

References
5 C.F.R. 731.106

PERSONNEL SCREENING

organization-defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of rescreening
organization-defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of rescreening
name: PS-3

statement

item
name: PS-3a.

Screen individuals prior to authorizing access to the system; and

item
name: PS-3b.

Rescreen individuals in accordance with .

guidance

Personnel screening and rescreening activities reflect applicable laws, Executive Orders, directives, regulations, policies, standards, guidelines, and specific criteria established for the risk designations of assigned positions. Organizations may define different rescreening conditions and frequencies for personnel accessing systems based on types of information processed, stored, or transmitted by the systems.

CLASSIFIED INFORMATION

name: PS-3 (1)

statement

Verify that individuals accessing a system processing, storing, or transmitting classified information are cleared and indoctrinated to the highest classification level of the information to which they have access on the system.

guidance

None.

FORMAL INDOCTRINATION

name: PS-3 (2)

statement

Verify that individuals accessing a system processing, storing, or transmitting types of classified information which require formal indoctrination, are formally indoctrinated for all the relevant types of information to which they have access on the system.

guidance

Types of classified information requiring formal indoctrination include, for example, Special Access Program (SAP), Restricted Data (RD), and Sensitive Compartment Information (SCI).

INFORMATION WITH SPECIAL PROTECTION MEASURES

organization-defined additional personnel screening criteria
organization-defined additional personnel screening criteria

name: PS-3 (3)

statement

Verify that individuals accessing a system processing, storing, or transmitting information requiring special protection:

item

name: PS-3 (3)(a)

Have valid access authorizations that are demonstrated by assigned official government duties; and

item

name: PS-3 (3)(b)

Satisfy .

guidance

Organizational information requiring special protection includes, for example, Controlled Unclassified Information (CUI). Personnel security criteria include, for example, position sensitivity background screening requirements.
None

CITIZENSHIP REQUIREMENTS

organization-defined information types
organization-defined information types

organization-defined citizenship requirements
organization-defined citizenship requirements
name: PS-3 (4)

statement

Verify that individuals accessing a system processing, storing, or transmitting meet .

guidance

None.
None

References

FIPS Publication 199
FIPS Publication 201
NIST Special Publication 800-73
NIST Special Publication 800-76
NIST Special Publication 800-78

PERSONNEL TERMINATION

organization-defined time-period
organization-defined time-period

organization-defined information security topics
organization-defined information security topics

organization-defined personnel or roles
organization-defined personnel or roles

organization-defined time-period
organization-defined time-period
name: PS-4

statement

Upon termination of individual employment:

item
name: PS-4a.

Disable system access within ;

item
name: PS-4b.

Terminate or revoke any authenticators and credentials associated with the individual;

item
name: PS-4c.

Conduct exit interviews that include a discussion of ;

item
name: PS-4d.

Retrieve all security-related organizational system-related property;

item
name: PS-4e.

Retain access to organizational information and systems formerly controlled by terminated individual; and

item
name: PS-4f.

Notify within .

guidance

System-related property includes, for example, hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes. Exit interviews ensure that terminated individuals understand the security constraints imposed by being former employees and that proper accountability is achieved for system-related property. Security topics of interest at exit interviews can include, for example, reminding terminated individuals of nondisclosure agreements and potential limitations on future employment. Exit interviews may not be possible for some terminated individuals, for example, in cases related to job abandonment, illnesses, and unavailability of supervisors. Exit interviews are important for individuals with security clearances. Timely execution of termination actions is essential for individuals terminated for cause. In certain situations, organizations consider disabling the system accounts of individuals that are being terminated prior to the individuals being notified.

POST-EMPLOYMENT REQUIREMENTS

name: PS-4 (1)

statement

item
name: PS-4 (1)(a)

Notify terminated individuals of applicable, legally binding post-employment requirements for the protection of organizational information; and

item
name: PS-4 (1)(b)

Require terminated individuals to sign an acknowledgment of post-employment requirements as part of the organizational termination process.

guidance

Organizations consult with the Office of the General Counsel regarding matters of post-employment requirements on terminated individuals.
None

AUTOMATED NOTIFICATION

organization-defined personnel or roles
organization-defined personnel or roles
name: PS-4 (2)

statement

Employ automated mechanisms to notify upon termination of an individual.

guidance

In organizations with many employees, not all personnel who need to know about termination actions receive the appropriate notifications#or, if such notifications are received, they may not occur in a timely manner. Automated mechanisms can be used to send automatic alerts or notifications to specific organizational personnel or roles when individuals are terminated. Such automatic alerts or notifications can be conveyed in a variety of ways, including, for example, telephonically, via electronic mail, via text message, or via websites.
None

PERSONNEL TRANSFER

organization-defined transfer or reassignment actions

organization-defined transfer or reassignment actions

organization-defined time-period following the formal transfer action
organization-defined time-period following the formal transfer action

organization-defined personnel or roles
organization-defined personnel or roles

organization-defined time-period
organization-defined time-period
name: PS-5

statement

item
name: PS-5a.

Review and confirm ongoing operational need for current logical and physical access authorizations to systems and facilities when individuals are reassigned or transferred to other positions within the organization;

item
name: PS-5b.

Initiate within ;

item
name: PS-5c.

Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and

item
name: PS-5d.

Notify within .

guidance

This control applies when reassignments or transfers of individuals are permanent or of such extended durations as to make the actions warranted. Organizations define actions appropriate for the types of reassignments or transfers, whether permanent or extended. Actions that may be required for personnel transfers or reassignments to other positions within organizations include, for example, returning old and issuing new keys, identification cards, and building passes; closing system accounts and establishing new accounts; changing system access authorizations (i.e., privileges); and providing for access to official records to which individuals had access at previous work locations and in previous system accounts.

ACCESS AGREEMENTS

organization-defined frequency
organization-defined frequency

organization-defined frequency
organization-defined frequency
name: PS-6

statement

item
name: PS-6a.

Develop and document access agreements for organizational systems;

item
name: PS-6b.

Review and update the access agreements ; and

item
name: PS-6c.

Verify that individuals requiring access to organizational information and systems:

item
name: PS-6c.1.

Sign appropriate access agreements prior to being granted access; and

item
name: PS-6c.2.

Re-sign access agreements to maintain access to organizational systems when access agreements have been updated or .

guidance

Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Signed access agreements include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with organizational systems to which access is authorized. Organizations can use electronic signatures to acknowledge access agreements unless specifically prohibited by organizational policy.

INFORMATION REQUIRING SPECIAL PROTECTION

name: PS-6 (1)

statement

Incorporated into PS-3.

CLASSIFIED INFORMATION REQUIRING SPECIAL PROTECTION

name: PS-6 (2)

statement

Verify that access to classified information requiring special protection is granted only to individuals who:

item
name: PS-6 (2)(a)

Have a valid access authorization that is demonstrated by assigned official government duties;

item
name: PS-6 (2)(b)

Satisfy associated personnel security criteria; and

item
name: PS-6 (2)(c)

Have read, understood, and signed a nondisclosure agreement.

guidance

Classified information requiring special protection includes, for example, collateral information, Special Access Program (SAP) information, and Sensitive Compartmented Information (SCI). Personnel security criteria reflect applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines.
None

POST-EMPLOYMENT REQUIREMENTS

name: PS-6 (3)

statement

item
name: PS-6 (3)(a)

Notify individuals of applicable, legally binding post-employment requirements for protection of organizational information; and

item
name: PS-6 (3)(b)

Require individuals to sign an acknowledgment of these requirements, if applicable, as part of granting initial access to covered information.

guidance

Organizations consult with the Office of the General Counsel regarding matters of post-employment requirements on terminated individuals.

EXTERNAL PERSONNEL SECURITY

organization-defined personnel or roles
organization-defined personnel or roles

organization-defined time-period
organization-defined time-period
name: PS-7

statement

item
name: PS-7a.

Establish personnel security requirements including security roles and responsibilities for external providers;

item
name: PS-7b.

Require external providers to comply with personnel security policies and procedures established by the organization;

item
name: PS-7c.

Document personnel security requirements;

item
name: PS-7d.

Require external providers to notify of any personnel transfers or terminations of external personnel who possess organizational credentials and/or badges, or who have system privileges within ; and

item
name: PS-7e.

Monitor provider compliance.

guidance

External provider refers to organizations other than the organization operating or acquiring the system. External providers include, for example, service bureaus, contractors, and other organizations providing system development, information technology services, outsourced applications, testing/assessment services, and network and security management. Organizations explicitly include personnel security requirements in acquisition-related documents. External providers may have personnel working at organizational facilities with credentials, badges, or system privileges issued by organizations. Notifications of external personnel changes ensure appropriate termination of privileges and credentials. Organizations define the transfers and terminations deemed reportable by security-related characteristics that include, for example, functions, roles, and nature of credentials/privileges associated with individuals transferred or terminated.

References

NIST Special Publication 800-35

PERSONNEL SANCTIONS

organization-defined personnel or roles
organization-defined personnel or roles

organization-defined time-period
organization-defined time-period
name: PS-8

statement

item
name: PS-8a.

Employ a formal sanctions process for individuals failing to comply with established information security policies and procedures; and

item
name: PS-8b.

Notify within when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

guidance

Organizational sanctions processes reflect applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines. Sanctions processes are described in access agreements and can be included as part of general personnel policies and procedures for

organizations. Organizations consult with the Office of the General Counsel regarding matters of employee sanctions.
All XX-1 Controls

RISK ASSESSMENT

RISK ASSESSMENT POLICY AND PROCEDURES

organization-defined personnel or roles
organization-defined personnel or roles

organization-defined senior management official
organization-defined senior management official

organization-defined frequency
organization-defined frequency

organization-defined frequency
organization-defined frequency
name: RA-1

statement

item
name: RA-1a.

Develop, document, and disseminate to :

item
name: RA-1a.1.

A risk assessment policy that:

item
name: RA-1a.1.(a)

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

item
name: RA-1a.1.(b)

Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and

item
name: RA-1a.2.

Procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls;

item
name: RA-1b.

Designate an to manage the risk assessment policy and procedures;

item
name: RA-1c.

Review and update the current risk assessment:

item
name: RA-1c.1.

Policy ; and

item
name: RA-1c.2.

Procedures ;

item
name: RA-1d.

Ensure that the risk assessment procedures implement the risk assessment policy and controls; and

item
name: RA-1e.

Develop, document, and implement remediation actions for violations of the risk assessment policy.

guidance

This control addresses the establishment of policy and procedures for the effective implementation of the controls and control enhancements in the RA family. The risk management strategy is an important factor in establishing policy and procedures. Comprehensive policy and procedures help provide security and privacy assurance. Security and privacy program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general security and privacy policy or can be represented by multiple policies reflecting the complex nature of organizations. The procedures can be established for security and privacy programs and for systems, if needed. Procedures describe how policies or controls are implemented and can be directed at the personnel or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. It is

important to recognize that restating controls does not constitute an organizational policy or procedure.

References

NIST Special Publication 800-12
NIST Special Publication 800-30
NIST Special Publication 800-39
NIST Special Publication 800-100

SECURITY CATEGORIZATION

name: RA-2

statement

item
name: RA-2a.

Categorize the system and information it processes, stores, and transmits;

item
name: RA-2b.

Document the security categorization results including supporting rationale, in the security plan for the system; and

item
name: RA-2c.

Verify that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.

guidance

Clearly defined authorization boundaries are a prerequisite for effective security categorization decisions. Security categories describe the potential adverse impacts to organizational operations, organizational assets, and individuals if organizational information and systems are comprised through a loss of confidentiality, integrity, or availability. Organizations conduct the security categorization process as an organization-wide activity with the involvement of Chief Information Officers, Senior Agency Information Security Officers, system owners, mission and business owners, and information owners/stewards. Organizations also consider the potential adverse impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level adverse impacts. Security categorization processes facilitate the development of inventories of information assets, and along with CM-8, mappings to specific system components where information is processed, stored, or transmitted.

SECOND-LEVEL CATEGORIZATION

name: RA-2 (1)

statement

Conduct a second-level categorization of organizational systems to obtain additional granularity on system impact levels.

guidance

Organizations apply the #high water mark# concept to each of their systems categorized in accordance with FIPS Publication 199. This process results in systems designated as low impact, moderate impact, or high impact. Organizations desiring additional granularity in the system impact designations for risk-based decision making, can further partition the systems into sub-categories of the initial, first-level system categorization. For example, a second-level categorization on a moderate-impact system can produce three new sub-categories: low-moderate systems, moderate-moderate systems, and high-moderate systems. This secondary categorization and the resulting sub-categories of the system give organizations an opportunity to further prioritize their investments related to security control selection and the tailoring of control baselines in responding to identified risks. Second-level categorization can also be used to determine those systems that are exceptionally critical to organizational missions and business operations. These systems are sometimes described as high-value assets and thus, organizations may be more focused on complexity, aggregation, and interconnections. Such systems can be identified by partitioning high-impact systems into low-high systems, moderate-high systems, and high-high systems.
None

References

FIPS Publication 199
FIPS Publication 200
NIST Special Publication 800-30
NIST Special Publication 800-39

RISK ASSESSMENT

organization-defined document
organization-defined document

organization-defined frequency
organization-defined frequency

organization-defined personnel or roles
organization-defined personnel or roles

organization-defined frequency
organization-defined frequency
name: RA-3

statement

item
name: RA-3a.

Conduct a risk assessment, including the likelihood and magnitude of harm, from:

item
name: RA-3a.1.

The unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and

item
name: RA-3a.2.

Privacy-related problems for individuals arising from the intentional processing of personally identifiable information;

item
name: RA-3b.

Integrate risk assessment results and risk management decsions from the organization and missions/business process perspectives with system-level risk assessments;

item
name: RA-3c.

Document risk assessment results in [Selection: security and privacy plans; risk assessment report;];

item
name: RA-3d.

Review risk assessment results ;

item
name: RA-3e.

Disseminate risk assessment results to ; and

item
name: RA-3f.

Update the risk assessment or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.

guidance

Clearly defined authorization boundaries are a prerequisite for effective risk assessments. Risk assessments consider threats, vulnerabilities, likelihood, and impact to organizational operations and assets, individuals, other organizations, and the Nation based on the operation and use of systems. Risk assessments also take into account risk from external parties including, for example, individuals accessing organizational systems; contractors operating systems on behalf of the organization; service providers; and outsourcing entities. Organizations can conduct risk assessments, either formal or informal, at all three tiers in the risk management hierarchy (i.e., organization level, mission/business process level, or system level) and at any phase in the system development life cycle. Risk assessments can also be conducted at various steps in the Risk Management Framework, including categorization, control selection, control implementation, control assessment, system authorization, and control monitoring. In addition to the information processed, stored, and transmitted by the system, risk assessments can also address any information related to the system including, for example, system design, the intended use of the system, testing results, and other supply chain-related information or artifacts. Assessments of risk can play an important role in security and privacy control selection processes, particularly during the application of tailoring guidance.

SUPPLY CHAIN RISK ASSESSMENT

organization-defined systems, system components, and system services
organization-defined systems, system components, and system services

organization-defined frequency
organization-defined frequency
name: RA-3 (1)

statement

item
name: RA-3 (1)(a)

Assess supply chain risks associated with ; and

item
name: RA-3 (1)(b)

Update the supply chain risk assessment , when there are significant changes to the relevant supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in the supply chain.

guidance

Supply chain-related events include, for example, disruption, theft, use of defective components, insertion of counterfeits, malicious development practices, improper delivery practices, and

insertion of malicious code. These events can have a significant impact on the confidentiality, integrity, or availability of a system and its information and therefore, can also adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. The supply chain-related events may be unintentional or malicious and can occur at any point during the system life cycle. An analysis of supply chain risk can help an organization identify systems or components for which additional supply chain risk mitigations are required.

References

NIST Special Publication 800-30
NIST Special Publication 800-39
NIST Special Publication 800-161

RISK ASSESSMENT UPDATE

name: RA-4

statement

Incorporated into RA-3.

VULNERABILITY SCANNING

organization-defined frequency and/or randomly in accordance with organization-defined process
organization-defined frequency and/or randomly in accordance with organization-defined process

organization-defined response times
organization-defined response times

organization-defined personnel or roles
organization-defined personnel or roles

name: RA-5

statement

item

name: RA-5a.

Scan for vulnerabilities in the system and hosted applications and when new vulnerabilities potentially affecting the system are identified and reported;

item

name: RA-5b.

Employ vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:

item
name: RA-5b.1.

Enumerating platforms, software flaws, and improper configurations;

item
name: RA-5b.2.

Formatting checklists and test procedures; and

item
name: RA-5b.3.

Measuring vulnerability impact;

item
name: RA-5c.

Analyze vulnerability scan reports and results from control assessments;

item
name: RA-5d.

Remediate legitimate vulnerabilities in accordance with an organizational assessment of risk;

item
name: RA-5e.

Share information obtained from the vulnerability scanning process and control assessments with to help eliminate similar vulnerabilities in other systems; and

item
name: RA-5f.

Employ vulnerability scanning tools that include the capability to readily update the vulnerabilities to be scanned.

guidance

Security categorization of information and systems guides the frequency and comprehensiveness of vulnerability scans. Organizations determine the required vulnerability scanning for system components, ensuring that the potential sources of vulnerabilities such as networked printers, scanners, and copiers are not overlooked. The vulnerabilities to be scanned need to be readily updated as new vulnerabilities are discovered, announced, and scanning methods developed. This process helps to ensure that potential vulnerabilities in the system are identified and

addressed as quickly as possible. Vulnerability analyses for custom software may require additional approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Organizations can use these analysis approaches in source code reviews and in a variety of tools including, for example, web-based application scanners, static analysis tools, and binary analyzers. Vulnerability scanning includes, for example, scanning for patch levels; scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and scanning for improperly configured or incorrectly operating information flow control mechanisms. Scanning tools that facilitate interoperability include, for example, products that are Security Content Automated Protocol (SCAP) validated. Thus, organizations consider using scanning tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that use the Open Vulnerability Assessment Language (OVAL) to determine the presence of vulnerabilities. Sources for vulnerability information include, for example, the Common Weakness Enumeration (CWE) listing and the National Vulnerability Database (NVD). Control assessments such as red team exercises provide additional sources of potential vulnerabilities for which to scan. Organizations also consider using scanning tools that express vulnerability impact by the Common Vulnerability Scoring System (CVSS).

UPDATE TOOL CAPABILITY

name: RA-5 (1)

statement

Incorporated into RA-5.

UPDATE BY FREQUENCY, PRIOR TO NEW SCAN, OR WHEN IDENTIFIED

organization-defined frequency
organization-defined frequency
name: RA-5 (2)

statement

Update the system vulnerabilities to be scanned [Selection (one or more): ; prior to a new scan; when new vulnerabilities are identified and reported].

guidance

None.

BREADTH AND DEPTH OF COVERAGE

name: RA-5 (3)

statement

Employ vulnerability scanning procedures that can identify the breadth and depth of coverage.

guidance

The identification of the breadth and depth of coverage can include, for example, the system components scanned and the vulnerabilities checked.
None

DISCOVERABLE INFORMATION

organization-defined corrective actions
organization-defined corrective actions
name: RA-5 (4)

statement

Determine unintended discoverable information about the system and take .

guidance

Discoverable information includes information that adversaries could obtain without directly compromising or breaching the system, for example, by collecting information the system is exposing or by conducting extensive searches of the web. Corrective actions can include, for example, notifying appropriate organizational personnel, removing designated information, or changing the system to make designated information less relevant or attractive to adversaries.

PRIVILEGED ACCESS

organization-identified system components
organization-identified system components

organization-defined vulnerability scanning activities
organization-defined vulnerability scanning activities
name: RA-5 (5)

statement

Implements privileged access authorization to for .

guidance

In certain situations, the nature of the vulnerability scanning may be more intrusive or the system component that is the subject of the scanning may contain classified or controlled unclassified information. Privileged access authorization to selected system components facilitates more thorough vulnerability scanning and protects the sensitive nature of such scanning.
None

AUTOMATED TREND ANALYSES

name: RA-5 (6)

statement

Employ automated mechanisms to compare the results of vulnerability scans over time to determine trends in system vulnerabilities.

guidance

None.
None

AUTOMATED DETECTION AND NOTIFICATION OF UNAUTHORIZED COMPONENTS

name: RA-5 (7)

statement

Incorporated into CM-8.

REVIEW HISTORIC AUDIT LOGS

name: RA-5 (8)

statement

Review historic audit logs to determine if a vulnerability identified in the system has been previously exploited.

guidance

None.

PENETRATION TESTING AND ANALYSES

name: RA-5 (9)

statement

Incorporated into CA-8.

CORRELATE SCANNING INFORMATION

name: RA-5 (10)

statement

Correlate the output from vulnerability scanning tools to determine the presence of multi-vulnerability and multi-hop attack vectors.

guidance

None.
None

References

NIST Special Publication 800-40
NIST Special Publication 800-70

NIST Special Publication 800-115

TECHNICAL SURVEILLANCE COUNTERMEASURES SURVEY

organization-defined locations
organization-defined locations

organization-defined frequency
organization-defined frequency

organization-defined events or indicators occur
organization-defined events or indicators occur
name: RA-6

statement

Employ a technical surveillance countermeasures survey at [Selection (one or more): ;].

guidance

Technical surveillance countermeasures surveys are performed by qualified personnel. Organizations use such surveys to detect the presence of technical surveillance devices and hazards and to identify technical security weaknesses that could aid in the conduct of technical penetrations of surveyed facilities. In addition, technical surveillance countermeasures surveys provide evaluations of the technical security posture of organizations and facilities and include thorough visual, electronic, and physical examinations of surveyed facilities, both internally and externally. The surveys also provide useful input for organizational risk assessments and critical information regarding organizational exposure to potential adversaries.
None

RISK RESPONSE
name: RA-7

statement

Respond to findings from security and privacy assessments, monitoring, and audits.

guidance

Organizations have a variety of options for responding to risk including: mitigating the risk by implementing new controls or strengthening existing controls; accepting the risk with appropriate justification or rationale; sharing or transferring the risk; or rejecting the risk. Organizational risk tolerance influences risk response decisions and actions. Risk response is also known as risk treatment. This control addresses the need to determine an appropriate

response to risk before a plan of action and milestones entry is generated. For example, the response may be to accept risk or reject risk, or it may be possible to mitigate the risk immediately so a plan of action and milestones entry is not needed. However, if the risk response is to mitigate the risk and the mitigation cannot be completed immediately, a plan of action and milestones entry is generated.

References

FIPS Publication 199
FIPS Publication 200
NIST Special Publication 800-30
NIST Special Publication 800-37
NIST Special Publication 800-39

PRIVACY IMPACT ASSESSMENTS

name: RA-8

statement

Conduct privacy impact assessments for systems, programs, or other activities that pose a privacy risk before:

item
name: RA-8a.

Developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form; and

item
name: RA-8b.

Initiating a new collection of information that:

item
name: RA-8b.1.

Will be collected, maintained, or disseminated using information technology; and

item
name: RA-8b.2.

Includes information in an identifiable form permitting the physical or online contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, ten or more persons, other than agencies, instrumentalities, or employees of the Federal Government.

guidance

Privacy impact assessments are an analysis of how information is managed to ensure that such management conforms to applicable legal, regulatory, and policy requirements regarding privacy; to determine the associated privacy risks and effects of creating, collecting, using, processing, storing, maintaining, disseminating, disclosing, and disposing of information in identifiable form in a system; and to examine and evaluate the protections and alternate processes for managing information to mitigate potential privacy concerns. A privacy impact assessment is an analysis and a formal document detailing the process and outcome of the analysis. To conduct the analysis, organizations use risk assessment processes. Although privacy impact assessments may be required by law, organizations may develop policies to require privacy impact assessments in circumstances where a privacy impact assessment would not be required by law.

CRITICALITY ANALYSIS

organization-defined systems, system components, or system services
organization-defined systems, system components, or system services

organization-defined decision points in the system development life cycle
organization-defined decision points in the system development life cycle
name: RA-9

statement

Identify critical system components and functions by performing a criticality analysis for at .

guidance

Not all system components, functions, or services necessarily require significant protections. Criticality analysis is a key tenet of, for example, supply chain risk management, and informs the prioritization of protection activities. The identification of critical system components and functions considers applicable regulations, directives, policies, standards, and guidelines, system functionality requirements, system and component interfaces, and system and component dependencies. Systems engineers conduct an end-to-end functional decomposition of a system to identify mission-critical functions and components. The functional decomposition includes the identification of core organizational missions supported by the system, decomposition into the specific functions to perform those missions, and traceability to the hardware, software, and firmware components that implement those functions, including when the functions are shared by many components within and beyond the system boundary. The operational environment of a system or component may impact the criticality including, for example, the connections to and dependencies on cyber-physical systems, devices, system-of-systems, and outsourced IT services. System components that allow unmediated access to critical system components or functions are considered critical due to the inherent vulnerabilities such components create. Component and function criticality are assessed in terms of the impact of a component or

function failure on the organizational missions supported by the system containing those components and functions. A criticality analysis is performed when an architecture or design is being developed, modified, or upgraded. If done early in the system life cycle, organizations may consider modifying the system design to reduce the critical nature of these components and functions by, for example, adding redundancy or alternate paths into the system design.

SYSTEM AND SERVICES ACQUISITION

SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES

organization-defined personnel or roles
organization-defined personnel or roles

organization-defined senior management official
organization-defined senior management official

organization-defined frequency
organization-defined frequency

organization-defined frequency
organization-defined frequency
name: SA-1

statement

item
name: SA-1a.

Develop, document, and disseminate to :

item
name: SA-1a.1.

A system and services acquisition policy that:

item
name: SA-1a.1.(a)

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

item
name: SA-1a.1.(b)

Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and

item
name: SA-1a.2.

Procedures to facilitate the implementation of the system and services acquisition policy and the associated system and services acquisition controls;

item
name: SA-1b.

Designate an to manage the system and services acquisition policy and procedures;

item
name: SA-1c.

Review and update the current system and services acquisition:

item
name: SA-1c.1.

Policy ; and

item
name: SA-1c.2.

Procedures ;

item
name: SA-1d.

Ensure that the system and services acquisition procedures implement the system and services acquisition policy and controls; and

item
name: SA-1e.

Develop, document, and implement remediation actions for violations of the system and services acquisition policy.

guidance

This control addresses the establishment of policy and procedures for the effective implementation of the controls and control enhancements in the SA family. The risk management strategy is an important factor in establishing policy and procedures. Comprehensive policy and procedures help provide security and privacy assurance. Security and privacy program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general security and privacy policy or can be represented by multiple policies reflecting the complex nature of organizations. The procedures can be established for security and privacy programs and for systems, if needed. Procedures describe how policies or controls are implemented and

can be directed at the personnel or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. It is important to recognize that restating controls does not constitute an organizational policy or procedure.

References

NIST Special Publication 800-12
NIST Special Publication 800-30
NIST Special Publication 800-39
NIST Special Publication 800-100

ALLOCATION OF RESOURCES

name: SA-2

statement

item
name: SA-2a.

Determine information security and privacy requirements for the system or system service in mission and business process planning;

item
name: SA-2b.

Determine, document, and allocate the resources required to protect the system or system service as part of the organizational capital planning and investment control process; and

item
name: SA-2c.

Establish a discrete line item for information security and privacy in organizational programming and budgeting documentation.

guidance

Resource allocation for information security and privacy includes funding for system or service acquisition, sustainment, and supply chain concerns throughout the system development life cycle.

References

NIST Special Publication 800-65

SYSTEM DEVELOPMENT LIFE CYCLE

organization-defined system development life cycle
organization-defined system development life cycle
name: SA-3

statement

item
name: SA-3a.

Manage the system using that incorporates information security and privacy considerations;

item
name: SA-3b.

Define and document information security and privacy roles and responsibilities throughout the system development life cycle;

item
name: SA-3c.

Identify individuals having information security and privacy roles and responsibilities; and

item
name: SA-3d.

Integrate the organizational information security and privacy risk management process into system development life cycle activities.

guidance

A system development life cycle process provides the foundation for the successful development, implementation, and operation of organizational systems. To apply the required security and privacy controls within the system development life cycle requires a basic understanding of information security and privacy, threats, vulnerabilities, adverse impacts, and risk to critical missions and business functions. The security engineering principles in SA-8 help individuals properly design, code, and test systems and system components. Organizations include qualified personnel including, for example, chief information security officers, security architects, security engineers, system security officers, and chief privacy officers in system development life cycle processes to ensure that established security and privacy requirements are incorporated into organizational systems. It is also important that developers include individuals on the development team that possess the requisite security and privacy expertise and skills to ensure that the needed security and privacy capabilities are effectively integrated into the system. Role-based security and privacy training programs can ensure that individuals having key security and privacy roles and responsibilities have the experience, skills, and expertise

to conduct assigned system development life cycle activities. The effective integration of security and privacy requirements into enterprise architecture also ensures that important security and privacy considerations are addressed early in the system life cycle and that those considerations are directly related to organizational mission and business processes. This process also facilitates the integration of the information security and privacy architectures into the enterprise architecture, consistent with risk management strategy of the organization. Because the development life cycle of a system involves multiple organizations, including, for example, external suppliers, developers, integrators, and service providers, it is important to recognize that acquisition and supply chain risk management functions and controls play a significant role in the overall effective management of the system during that life cycle.

MANAGE DEVELOPMENT ENVIRONMENT

name: SA-3 (1)

statement

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

guidance

None.

USE OF LIVE DATA

name: SA-3 (2)

statement

item

name: SA-3 (2)(a)

Approve, document, and control the use of live data in development, test, and integration environments for the system, system component, or system service; and

item

name: SA-3 (2)(b)

Ensure development, test, and integration environments for the system, system component, or system service are protected at the same impact or classification level as any live data used.

guidance

Live data is also referred to as operational data. The use of live data in preproduction environments can result in significant risk to organizations. Organizations can minimize such risk by using test or dummy data during the design, development, and testing of systems, system components, and system services.

TECHNOLOGY REFRESH

name: SA-3 (3)

statement

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

guidance

Technology refresh planning may encompass hardware, software, firmware, processes, personnel skill sets, suppliers, service providers, and facilities. The use of obsolete or nearing obsolete technology may increase security and privacy risks associated with, for example, unsupported components, components unable to implement security or privacy requirements, counterfeit or re-purposed components, slow or inoperable components, components from untrusted sources, inadvertent personnel error, or increased complexity.
None

References

NIST Special Publication 800-30
NIST Special Publication 800-37
NIST Special Publication 800-64

ACQUISITION PROCESS

name: SA-4

statement

Include the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the system, system component, or system service:

item

name: SA-4a.

Security and privacy functional requirements;

item

name: SA-4b.

Strength of mechanism requirements;

item

name: SA-4c.

Security and privacy assurance requirements;

item

name: SA-4d.

Security and privacy documentation requirements;

item
name: SA-4e.

Requirements for protecting security and privacy documentation;

item
name: SA-4f.

Description of the system development environment and environment in which the system is intended to operate;

item
name: SA-4g.

Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; and

item
name: SA-4h.

Acceptance criteria.

guidance

System components are discrete, identifiable information technology assets including, for example, hardware, software, or firmware. These components represent the building blocks of a system. System components typically consist of commercial information technology products. Security and privacy functional requirements include security and privacy capabilities, functions, and mechanisms. Strength requirements associated with such capabilities, functions, and mechanisms include degree of correctness, completeness, resistance to tampering or bypass, and resistance to direct attack. Security and privacy assurance requirements include development processes, procedures, practices, and methodologies; and the evidence from development and assessment activities providing grounds for confidence that the required security and privacy functionality is implemented and possesses the required strength of mechanism. Security and privacy documentation requirements address all phases of the system development life cycle. Security and privacy requirements are expressed in terms of security and privacy controls and control enhancements that have been selected through the tailoring process. The tailoring process includes, for example, the specification of parameter values using assignment and selection statements and platform dependencies and implementation information. Security and privacy documentation provides user and administrator guidance regarding the implementation and operation of security and privacy controls. The level of detail required in such documentation is based on the security categorization or classification level of the system and the degree to which organizations depend on the stated security or privacy capabilities, functions, or mechanisms to

meet overall risk response expectations. Security and privacy requirements can include mandated configuration settings specifying allowed functions, ports, protocols, and services. Acceptance criteria for systems, system components, and system services are defined in the same manner as such criteria for any organizational acquisition or procurement.

FUNCTIONAL PROPERTIES OF CONTROLS

name: SA-4 (1)

statement

Require the developer of the system, system component, or system service to provide a description of the functional properties of the controls to be implemented.

guidance

Functional properties of security and privacy controls describe the functionality (i.e., security or privacy capability, functions, or mechanisms) visible at the interfaces of the controls and specifically exclude functionality and data structures internal to the operation of the controls.
None

DESIGN AND IMPLEMENTATION INFORMATION FOR CONTROLS

organization-defined design and implementation information
organization-defined design and implementation information

organization-defined level of detail
organization-defined level of detail

name: SA-4 (2)

statement

Require the developer of the system, system component, or system service to provide design and implementation information for the selected controls that includes: [Selection (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics;] at .

guidance

Organizations may require different levels of detail in design and implementation documentation for controls implemented in organizational systems, system components, or system services based on mission and business requirements; requirements for trustworthiness and resiliency; and requirements for analysis and testing. Systems can be partitioned into multiple subsystems. Each subsystem within the system can contain one or more modules. The high-level design for the system is expressed in terms of subsystems and the interfaces between subsystems providing security-relevant functionality. The low-level design for the system is expressed in terms of modules and the interfaces between modules providing security-relevant functionality. Design

and implementation documentation may include information such as manufacturer, version, serial number, verification hash signature, software libraries used, date of purchase or download, and the vendor or download source. Source code and hardware schematics are referred to as the implementation representation of the system.
None

DEVELOPMENT METHODS, TECHNIQUES, AND PRACTICES

organization-defined systems engineering methods; Selection (one or more): systems security engineering methods; privacy engineering methods
organization-defined systems engineering methods; Selection (one or more): systems security engineering methods; privacy engineering methods
name: SA-4 (3)

statement

Require the developer of the system, system component, or system service to demonstrate the use of a system development life cycle process that includes ; software development methods; testing, evaluation, assessment, verification, and validation methods; and quality control processes].

guidance

Following a system development life cycle that includes state-of-the-practice software development methods, systems engineering methods, systems security and privacy engineering methods, and quality control processes helps to reduce the number and severity of latent errors within systems, system components, and system services. Reducing the number and severity of such errors reduces the number of vulnerabilities in those systems, components, and services.
None

ASSIGNMENT OF COMPONENTS TO SYSTEMS

name: SA-4 (4)
CM-8(9)

statement

Incorporated into CM-8(9).

SYSTEM, COMPONENT, AND SERVICE CONFIGURATIONS

organization-defined security configurations
organization-defined security configurations
name: SA-4 (5)

statement

Require the developer of the system, system component, or system service to:

item
name: SA-4 (5)(d)

Deliver the system, component, or service with implemented; and

item
name: SA-4 (5)(e)

Use the configurations as the default for any subsequent system, component, or service reinstallation or upgrade.

guidance

Security configurations include, for example, the U.S. Government Configuration Baseline (USGCB) and any limitations on functions, ports, protocols, and services. Security characteristics include, for example, requiring that default passwords have been changed.
None

USE OF INFORMATION ASSURANCE PRODUCTS

name: SA-4 (6)

statement

item
name: SA-4 (6)(a)

Employ only government off-the-shelf or commercial off-the-shelf information assurance and information assurance-enabled information technology products that compose an NSA-approved solution to protect classified information when the networks used to transmit the information are at a lower classification level than the information being transmitted; and

item
name: SA-4 (6)(b)

Ensure that these products have been evaluated and/or validated by NSA or in accordance with NSA-approved procedures.

guidance

Commercial off-the-shelf IA or IA-enabled information technology products used to protect classified information by cryptographic means may be required to use NSA-approved key management.

NIAP-APPROVED PROTECTION PROFILES

name: SA-4 (7)

statement

item

name: SA-4 (7)(a)

Limit the use of commercially provided information assurance and information assurance-enabled information technology products to those products that have been successfully evaluated against a National Information Assurance partnership (NIAP)-approved Protection Profile for a specific technology type, if such a profile exists; and

item
name: SA-4 (7)(b)

Require, if no NIAP-approved Protection Profile exists for a specific technology type but a commercially provided information technology product relies on cryptographic functionality to enforce its security policy, that the cryptographic module is FIPS-validated or NSA-approved.

guidance

None.

CONTINUOUS MONITORING PLAN FOR CONTROLS

organization-defined level of detail
organization-defined level of detail
name: SA-4 (8)

statement

Require the developer of the system, system component, or system service to produce a plan for continuous monitoring of security and privacy control effectiveness that contains the following: .

guidance

The objective of continuous monitoring plans is to determine if the complete set of planned, required, and deployed security and privacy controls within the system, system component, or system service continue to be effective over time based on the inevitable changes that occur. Developer continuous monitoring plans include a sufficient level of detail such that the information can be incorporated into the continuous monitoring strategies and programs implemented by organizations.

FUNCTIONS, PORTS, PROTOCOLS, AND SERVICES IN USE

name: SA-4 (9)

statement

Require the developer of the system, system component, or system service to identify the functions, ports, protocols, and services intended for organizational use.

guidance

The identification of functions, ports, protocols, and services early in the system development life cycle, for example, during the initial requirements definition and design phases, allows organizations to influence the design of the system, system component, or system service. This early involvement in the system life cycle helps organizations to avoid or minimize the use of functions, ports, protocols, or services that pose unnecessarily high risks and understand the trade-offs involved in blocking specific ports, protocols, or services or when requiring system service providers to do so. Early identification of functions, ports, protocols, and services avoids costly retrofitting of controls after the system, component, or system service has been implemented. SA-9 describes the requirements for external system services with organizations identifying which functions, ports, protocols, and services are provided from external sources.

USE OF APPROVED PIV PRODUCTS

name: SA-4 (10)

statement

Employ only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational systems.

guidance

None.

References

ISO/IEC 15408
FIPS Publication 140-2
FIPS Publication 201
NIST Special Publication 800-23
NIST Special Publication 800-35
NIST Special Publication 800-36
NIST Special Publication 800-37
NIST Special Publication 800-64
NIST Special Publication 800-70
NIST Special Publication 800-73
NIST Special Publication 800-137
NIST Special Publication 800-161

SYSTEM DOCUMENTATION

organization-defined actions
organization-defined actions

organization-defined personnel or roles
organization-defined personnel or roles

name: SA-5

statement

item
name: SA-5a.

Obtain administrator documentation for the system, system component, or system service that describes:

item
name: SA-5a.1.

Secure configuration, installation, and operation of the system, component, or service;

item
name: SA-5a.2.

Effective use and maintenance of security and privacy functions and mechanisms; and

item
name: SA-5a.3.

Known vulnerabilities regarding configuration and use of administrative or privileged functions;

item
name: SA-5b.

Obtain user documentation for the system, system component, or system service that describes:

item
name: SA-5b.1.

User-accessible security and privacy functions and mechanisms and how to effectively use those functions and mechanisms;

item
name: SA-5b.2.

Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner and protect individual privacy; and

item
name: SA-5b.3.

User responsibilities in maintaining the security of the system, component, or service and privacy of individuals;

item
name: SA-5c.

Document attempts to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent and takes in response;

item
name: SA-5d.

Protect documentation as required, in accordance with the organizational risk management strategy; and

item
name: SA-5e.

Distribute documentation to .

guidance

This control helps organizational personnel understand the implementation and operation of security and privacy controls associated with systems, system components, and system services. Organizations consider establishing specific measures to determine the quality and completeness of the content provided. System documentation may be used, for example, to support the management of supply chain risk, incident response, and other functions. Personnel or roles requiring documentation may include, for example, system owners, system security officers, and system administrators. Attempts to obtain documentation may include, for example, directly contacting manufacturers or suppliers and conducting web-based searches. The inability to obtain needed documentation may occur, for example, due to the age of the system or component or lack of support from developers and contractors. In those situations, organizations may need to recreate selected documentation if such documentation is essential to the implementation or operation of the security and privacy controls. The level of protection provided for the system, component, or service documentation is commensurate with the security category or classification of the system. Documentation that addresses system vulnerabilities may require an increased level of protection. Secure operation of the system, includes, for example, initially starting the system and resuming secure system operation after any lapse in system operation.

FUNCTIONAL PROPERTIES OF SECURITY CONTROLS

name: SA-5 (1)
SA-4(1)

statement

Incorporated into SA-4(1).

SECURITY-RELEVANT EXTERNAL SYSTEM INTERFACES

name: SA-5 (2)
SA-4(2)

statement

Incorporated into SA-4(2).

HIGH-LEVEL DESIGN

name: SA-5 (3)
SA-4(2)

statement

Incorporated into SA-4(2).

LOW-LEVEL DESIGN

name: SA-5 (4)
SA-4(2)

statement

Incorporated into SA-4(2).

SOURCE CODE

name: SA-5 (5)
SA-4(2)

statement

Incorporated into SA-4(2).

SOFTWARE USAGE RESTRICTIONS

name: SA-6

statement

Incorporated into CM-10 and SI-7.

USER-INSTALLED SOFTWARE

name: SA-7

statement

Incorporated into CM-11 and SI-7.

SECURITY AND PRIVACY ENGINEERING PRINCIPLES

organization-defined systems security engineering principles
organization-defined systems security engineering principles
name: SA-8

statement

Apply in the specification, design, development, implementation, and modification of the system and system components.

guidance

Organizations can apply systems security and privacy engineering principles to new systems under development or to systems undergoing upgrades. For legacy systems, organizations apply systems security and privacy engineering principles to system upgrades and modifications to the extent feasible, given the current state of hardware, software, and firmware components within those systems. The application of systems security and privacy engineering concepts and principles help to develop trustworthy, secure systems and system components and reduce the susceptibility of organizations to disruptions, hazards, threats, and creating privacy-related problems for individuals. Examples of these concepts and principles include, developing layered protections; establishing security and privacy policies, architecture, and controls as the foundation for design and development; incorporating security and privacy requirements into the system development life cycle; delineating physical and logical security boundaries; ensuring that developers are trained on how to build secure software; tailoring security and privacy controls to meet organizational and operational needs; performing threat modeling to identify use cases, threat agents, attack vectors and patterns, design patterns, and compensating controls needed to mitigate risk. Organizations that apply security and privacy engineering concepts and principles can facilitate the development of trustworthy, secure systems, system components, and system services; reduce risk to acceptable levels; and make informed risk management decisions. Security engineering principles can also be used to protect against certain supply chain risks including, for example, incorporating tamper-resistant hardware into a design.

References

FIPS Publication 199
FIPS Publication 200
NIST Special Publication 800-53A
NIST Special Publication 800-64

EXTERNAL SYSTEM SERVICES

organization-defined security and privacy controls
organization-defined security and privacy controls

organization-defined processes, methods, and techniques
organization-defined processes, methods, and techniques
name: SA-9

statement

item

name: SA-9a.

Require that providers of external system services comply with organizational security and privacy requirements and employ ;

item
name: SA-9b.

Define and document organizational oversight and user roles and responsibilities with regard to external system services; and

item
name: SA-9c.

Employ to monitor security and privacy control compliance by external service providers on an ongoing basis.

guidance

External system services are those services that are implemented external to authorization boundaries of organizational systems. This includes services that are used by, but not a part of, organizational systems. Organizations establish relationships with external service providers in a variety of ways including, for example, through business partnerships, contracts, interagency agreements, lines of business arrangements, licensing agreements, joint ventures, and supply chain exchanges. The responsibility for managing risks from the use of external system services remains with authorizing officials. For services external to organizations, a chain of trust requires that organizations establish and retain a level of confidence that each provider in the consumer-provider relationship provides adequate protection for the services rendered. The extent and nature of this chain of trust varies based on the relationships between organizations and the external providers. Organizations document the basis for trust relationships so the relationships can be monitored over time. External system services documentation includes government, service providers, end user security roles and responsibilities, and service-level agreements. Service-level agreements define expectations of performance for implemented security and privacy controls; describe measurable outcomes, and identify remedies and response requirements for identified instances of noncompliance.

RISK ASSESSMENTS AND ORGANIZATIONAL APPROVALS

organization-defined personnel or roles
organization-defined personnel or roles
name: SA-9 (1)

statement

item
name: SA-9 (1)(a)

Conduct an organizational assessment of risk prior to the acquisition or outsourcing of information security services; and

item
name: SA-9 (1)(b)

Verify that the acquisition or outsourcing of dedicated information security services is approved by .

guidance

Examples of information security services include the operation of security devices such as firewalls, or key management services; and incident monitoring, analysis and response. Risks assessed may include, for example, system-related, mission-related, privacy-related, or supply chain-related risks.

IDENTIFICATION OF FUNCTIONS, PORTS, PROTOCOLS, AND SERVICES

organization-defined external system services
organization-defined external system services
name: SA-9 (2)

statement

Require providers of to identify the functions, ports, protocols, and other services required for the use of such services.

guidance

Information from external service providers regarding the specific functions, ports, protocols, and services used in the provision of such services can be useful when the need arises to understand the trade-offs involved in restricting certain functions and services or blocking certain ports and protocols.

ESTABLISH AND MAINTAIN TRUST RELATIONSHIP WITH PROVIDERS

organization-defined security and privacy requirements, properties, factors, or conditions defining acceptable trust relationships
organization-defined security and privacy requirements, properties, factors, or conditions defining acceptable trust relationships
name: SA-9 (3)

statement

Establish, document, and maintain trust relationships with external service providers based on .

guidance

The degree of confidence that the risk from using external services is at an acceptable level depends on the trust that organizations place in the external providers, individually or in combination. Trust relationships can help organizations to gain increased levels of confidence that participating service providers are providing adequate protection for the services rendered. They can also be useful when conducting incident response or when planning for upgrades or obsolescence. Trust relationships can be complicated due to the number of potential entities participating in the consumer-provider interactions, subordinate relationships and levels of trust, and types of interactions between the parties. In some cases, the degree of trust is based on the level of control organizations can exert on external service providers regarding the controls necessary for the protection of the service, information, or individual privacy and the evidence brought forth as to the effectiveness of the implemented controls. The level of control is established by the terms and conditions of the contracts or service-level agreements. Extensive control may include negotiating contracts or agreements that specify security and privacy requirements for providers. Limited control may include using contracts or service-level agreements to obtain commodity services such as commercial telecommunications services.

CONSISTENT INTERESTS OF CONSUMERS AND PROVIDERS

organization-defined actions
organization-defined actions

organization-defined external service providers
organization-defined external service providers

name: SA-9 (4)

statement

Take to verify that the interests of are consistent with and reflect organizational interests.

guidance

As organizations increasingly use external service providers, it is possible that the interests of the service providers may diverge from organizational interests. In such situations, simply having the required technical, management, or operational controls in place may not be sufficient if the providers that implement and manage those controls are not operating in a manner consistent with the interests of the consuming organizations. The actions that organizations might take to address such concerns include, for example, requiring background checks for selected service provider personnel; examining ownership records; employing only trustworthy service providers, including providers with which organizations have had successful trust relationships; and conducting routine periodic, unscheduled visits to service provider facilities.

None

PROCESSING, STORAGE, AND SERVICE LOCATION

organization-defined locations
organization-defined locations

organization-defined requirements or conditions
organization-defined requirements or conditions
name: SA-9 (5)

statement

Restrict the location of [Selection (one or more): information processing; information or data; system services] to based on .

guidance

The location of information processing, information and data storage, or system services that are critical to organizations can have a direct impact on the ability of those organizations to successfully execute their missions and business functions. This occurs when external providers control the location of processing, storage, or services. The criteria that external providers use for the selection of processing, storage, or service locations may be different from the criteria organizations use. For example, organizations may desire that data or information storage locations are restricted to certain locations to help facilitate incident response activities in case of information security or privacy incidents. Such incident response activities including, for example, forensic analyses and after-the-fact investigations, may be adversely affected by the governing laws or protocols in the locations where processing and storage occur and/or the locations from which system services emanate.

ORGANIZATION-CONTROLLED CRYPTOGRAPHIC KEYS

name: SA-9 (6)

statement

Maintain exclusive control of cryptographic keys.

guidance

Maintaining exclusive control of cryptographic keys in an external system prevents decryption of organizational data by external system staff. This enhancement can be implemented, for example, by encrypting and decrypting data inside the organization as data is sent to and received from the external system or through use of a component that permits encryption and decryption functions to be local to the external system, but allows the organization exclusive access to encryption keys.

ORGANIZATION-CONTROLLED INTEGRITY CHECKING

name: SA-9 (7)

statement

Provide the capability to check the integrity of organizational information while it resides in the external system.

guidance

Storage of organizational information in an external system could limit organizational visibility into the security status of its data. The ability for the organization to verify and validate the integrity of its stored data without transferring it out of the external system provides such visibility.

References

NIST Special Publication 800-35
NIST Special Publication 800-161

DEVELOPER CONFIGURATION MANAGEMENT

organization-defined configuration items under configuration management
organization-defined configuration items under configuration management

organization-defined personnel
organization-defined personnel
name: SA-10

statement

Require the developer of the system, system component, or system service to:

item
name: SA-10a.

Perform configuration management during system, component, or service [Selection (one or more): design; development; implementation; operation; disposal];

item
name: SA-10b.

Document, manage, and control the integrity of changes to ;

item
name: SA-10c.

Implement only organization-approved changes to the system, component, or service;

item
name: SA-10d.

Document approved changes to the system, component, or service and the potential security and privacy impacts of such changes; and

item
name: SA-10e.

Track security flaws and flaw resolution within the system, component, or service and report findings to .

guidance

Organizations consider the quality and completeness of the configuration management activities conducted by developers as direct evidence of applying effective security controls. Controls include, for example, protecting from unauthorized modification or destruction, the master copies of material used to generate security-relevant portions of the system hardware, software, and firmware. Maintaining the integrity of changes to the system, system component, or system service requires strict configuration control throughout the system development life cycle to track authorized changes and to prevent unauthorized changes. The configuration items that are placed under configuration management include: the formal model; the functional, high-level, and low-level design specifications; other design data; implementation documentation; source code and hardware schematics; the current running version of the object code; tools for comparing new versions of security-relevant hardware descriptions and source code with previous versions; and test fixtures and documentation. Depending on the mission and business needs of organizations and the nature of the contractual relationships in place, developers may provide configuration management support during the operations and maintenance phases of the system life cycle.

SOFTWARE AND FIRMWARE INTEGRITY VERIFICATION

name: SA-10 (1)

statement

Require the developer of the system, system component, or system service to enable integrity verification of software and firmware components.

guidance

This control enhancement allows organizations to detect unauthorized changes to software and firmware components using developer-provided tools, techniques, and mechanisms. Integrity checking mechanisms can also address counterfeiting of software and firmware components. Organizations verify the integrity of software and firmware components, for example, through secure one-way hashes provided by developers. Delivered software and firmware components also include any updates to such components.

ALTERNATIVE CONFIGURATION MANAGEMENT PROCESSES

name: SA-10 (2)

statement

Provide an alternate configuration management process using organizational personnel in the absence of a dedicated developer configuration management team.

guidance

Alternate configuration management processes may be required, for example, when organizations use commercial off-the-shelf information technology products. Alternate configuration management processes include organizational personnel that review and approve proposed changes to systems, system components, and system services; and that conduct security and privacy impact analyses prior to the implementation of changes to systems, components, or services.
None

HARDWARE INTEGRITY VERIFICATION

name: SA-10 (3)

statement

Require the developer of the system, system component, or system service to enable integrity verification of hardware components.

guidance

This control enhancement allows organizations to detect unauthorized changes to hardware components using developer-provided tools, techniques, methods, and mechanisms. Organizations verify the integrity of hardware components, for example, with hard-to-copy labels and verifiable serial numbers provided by developers, and by requiring the implementation of anti-tamper technologies. Delivered hardware components also include updates to such components.

TRUSTED GENERATION

name: SA-10 (4)

statement

Require the developer of the system, system component, or system service to employ tools for comparing newly generated versions of security-relevant hardware descriptions, source code, and object code with previous versions.

guidance

This control enhancement addresses authorized changes to hardware, software, and firmware components between versions during development. The focus is on the efficacy of the configuration management process by the developer to ensure that newly generated versions of security-relevant hardware descriptions, source code, and object code continue to enforce the security policy for the system, system component, or system service. In contrast, SA-10(1)

and SA-10(3) allow organizations to detect unauthorized changes to hardware, software, and firmware components using tools, techniques, and/or mechanisms provided by developers.
None

MAPPING INTEGRITY FOR VERSION CONTROL

name: SA-10 (5)

statement

Require the developer of the system, system component, or system service to maintain the integrity of the mapping between the master build data (hardware drawings and software/ firmware code) describing the current version of security-relevant hardware, software, and firmware and the on-site master copy of the data for the current version.

guidance

This control enhancement addresses changes to hardware, software, and firmware components during initial development and during system life cycle updates. Maintaining the integrity between the master copies of security-relevant hardware, software, and firmware (including designs and source code) and the equivalent data in master copies on-site in operational environments is essential to ensure the availability of organizational systems supporting critical missions and business functions.
None

TRUSTED DISTRIBUTION

name: SA-10 (6)

statement

Require the developer of the system, system component, or system service to execute procedures for ensuring that security-relevant hardware, software, and firmware updates distributed to the organization are exactly as specified by the master copies.

guidance

The trusted distribution of security-relevant hardware, software, and firmware updates ensure that such updates are correct representations of the master copies maintained by the developer and have not been tampered with during distribution.
None

References

FIPS Publication 140-2
NIST Special Publication 800-128

DEVELOPER TESTING AND EVALUATION

organization-defined frequency
organization-defined frequency

organization-defined depth and coverage
organization-defined depth and coverage
name: SA-11

statement

Require the developer of the system, system component, or system service, at all post-design phases of the system development life cycle, to:

item
name: SA-11a.

Create and implement a security and privacy assessment plan;

item
name: SA-11b.

Perform [Selection (one or more): unit; integration; system; regression] testing/evaluation at ;

item
name: SA-11c.

Produce evidence of the execution of the assessment plan and the results of the testing and evaluation;

item
name: SA-11d.

Implement a verifiable flaw remediation process; and

item
name: SA-11e.

Correct flaws identified during testing and evaluation.

guidance

Developmental testing and evaluation confirms that the required security and privacy controls are implemented correctly, operating as intended, enforcing the desired security and privacy policies, and meeting established security and privacy requirements. Security properties of systems and the privacy of individuals may be affected by the interconnection of system components or changes to those components. These interconnections or changes including, for example, upgrading or replacing applications, operating systems, and firmware, may adversely

affect previously implemented security and privacy controls. This control provides additional types of testing and evaluation that developers can conduct to reduce or eliminate potential flaws. Testing custom software applications may require approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Developers can use these analysis approaches in a variety of tools and in source code reviews. Security and privacy assessment plans provide the specific activities that developers plan to carry out including the types of analyses, testing, evaluation, and reviews of software and firmware components, the degree of rigor to be applied, and the types of artifacts produced during those processes. The depth of testing and evaluation refers to the rigor and level of detail associated with the assessment process. The coverage of testing and evaluation refers to the scope (i.e., number and type) of the artifacts included in the assessment process. Contracts specify the acceptance criteria for security and privacy assessment plans, flaw remediation processes, and the evidence that the plans and processes have been diligently applied. Methods for reviewing and protecting assessment plans, evidence, and documentation are commensurate with the security category or classification level of the system. Contracts may specify documentation protection requirements.

STATIC CODE ANALYSIS

name: SA-11 (1)

statement

Require the developer of the system, system component, or system service to employ static code analysis tools to identify common flaws and document the results of the analysis.

guidance

Static code analysis provides a technology and methodology for security reviews and may include, for example, checking for weaknesses in the code and checking for incorporation of libraries or other included code with known vulnerabilities or that are out-of-date and not supported. Such analysis can be used to identify vulnerabilities and enforce secure coding practices. Static code analysis is most effective when used early in the development process, when each code change can be automatically scanned for potential weaknesses. Static analysis can provide clear remediation guidance along with defects to enable developers to fix such defects. Evidence of correct implementation of static analysis can include, for example, aggregate defect density for critical defect types; evidence that defects were inspected by developers or security professionals; and evidence that defects were remediated. An excessively high density of ignored findings, commonly referred to as false positives, indicates a potential problem with the analysis process or the analysis tool. In such cases, organizations weigh the validity of the evidence against evidence from other sources.

None

THREAT MODELING AND VULNERABILITY ANALYSES

organization-defined breadth and depth
organization-defined breadth and depth

organization-defined information concerning impact, environment of operations, known or assumed threats, and acceptable risk levels
organization-defined information concerning impact, environment of operations, known or assumed threats, and acceptable risk levels

organization-defined tools and methods
organization-defined tools and methods

organization-defined acceptance criteria
organization-defined acceptance criteria
name: SA-11 (2)

statement

Require the developer of the system, system component, or system service to perform threat modeling and vulnerability analyses at during development and during the subsequent testing and evaluation of the system, component, or service that:

item
name: SA-11 (2)(a)

Uses ;

item
name: SA-11 (2)(b)

Employs ; and

item
name: SA-11 (2)(c)

Produces evidence that meets .

guidance

Systems, system components, and system services may deviate significantly from the functional and design specifications created during the requirements and design phases of the system development life cycle. Therefore, threat modeling and vulnerability analyses of those systems, system components, and system services prior to delivery are critical to the effective operation of those systems, components, and services. Threat modeling and vulnerability analyses at this phase of the system development life cycle ensure that design and implementation changes have been accounted for and vulnerabilities created because of those changes have been reviewed and mitigated. Related controls: PM-15, RA-3, RA-5.

INDEPENDENT VERIFICATION OF ASSESSMENT PLANS AND EVIDENCE

organization-defined independence criteria
organization-defined independence criteria
name: SA-11 (3)

statement

item
name: SA-11 (3)(a)

Require an independent agent satisfying to verify the correct implementation of the developer security and privacy assessment plans and the evidence produced during testing and evaluation; and

item
name: SA-11 (3)(b)

Verify that the independent agent is provided with sufficient information to complete the verification process or granted the authority to obtain such information.

guidance

Independent agents have the necessary qualifications, including the expertise, skills, training, certifications, and experience, to verify the correct implementation of developer security and privacy assessment plans.

MANUAL CODE REVIEWS

organization-defined specific code
organization-defined specific code

organization-defined processes, procedures, and/or techniques
organization-defined processes, procedures, and/or techniques
name: SA-11 (4)

statement

Require the developer of the system, system component, or system service to perform a manual code review of using .

guidance

Manual code reviews are usually reserved for the critical software and firmware components of systems. Such code reviews are effective in identifying weaknesses that require knowledge of the application#s requirements or context which in most cases, are unavailable to automated analytic

tools and techniques including static and dynamic analysis. Components benefiting from manual review include, for example, verifying access control matrices against application controls and reviewing more detailed aspects of cryptographic implementations and controls.
None

PENETRATION TESTING

organization-defined breadth and depth
organization-defined breadth and depth

organization-defined constraints
organization-defined constraints

name: SA-11 (5)

statement

Require the developer of the system, system component, or system service to perform penetration testing at and with .

guidance

Penetration testing is an assessment methodology in which assessors, using all available information technology product or system documentation and working under specific constraints, attempt to circumvent implemented security and privacy features of information technology products and systems. Useful information for assessors conducting penetration testing can include, for example, product and system design specifications, source code, and administrator and operator manuals. Penetration testing can include white-box, gray-box, or black box testing with associated analyses performed by skilled professionals simulating adversary actions. The objective of penetration testing is to uncover the potential vulnerabilities in systems, system components and services resulting from implementation errors, configuration faults, or other operational weaknesses or deficiencies. Penetration tests can be performed in conjunction with automated and manual code reviews to provide greater levels of analysis than would ordinarily be possible.

ATTACK SURFACE REVIEWS

name: SA-11 (6)

statement

Require the developer of the system, system component, or system service to perform attack surface reviews.

guidance

Attack surfaces of systems and system components are exposed areas that make those systems more vulnerable to attacks. This includes any accessible areas where weaknesses or deficiencies in the hardware, software, and firmware components provide opportunities for adversaries to

exploit vulnerabilities. Attack surface reviews ensure that developers analyze the design and implementation changes to systems and mitigate attack vectors generated as a result of the changes. Correction of identified flaws includes, for example, deprecation of unsafe functions.
None

VERIFY SCOPE OF TESTING AND EVALUATION

organization-defined depth of testing and evaluation
organization-defined depth of testing and evaluation
name: SA-11 (7)

statement

Require the developer of the system, system component, or system service to verify that the scope of testing and evaluation provides complete coverage of required security and privacy controls at .

guidance

Verifying that testing and evaluation provides complete coverage of required security and privacy controls can be accomplished by a variety of analytic techniques ranging from informal to formal. Each of these techniques provides an increasing level of assurance corresponding to the degree of formality of the analysis. Rigorously demonstrating control coverage at the highest levels of assurance can be provided using formal modeling and analysis techniques including correlation between control implementation and corresponding test cases.
None

DYNAMIC CODE ANALYSIS

name: SA-11 (8)

statement

Require the developer of the system, system component, or system service to employ dynamic code analysis tools to identify common flaws and document the results of the analysis.

guidance

Dynamic code analysis provides run-time verification of software programs, using tools capable of monitoring programs for memory corruption, user privilege issues, and other potential security problems. Dynamic code analysis employs run-time tools to ensure that security functionality performs in the way it was designed. A specialized type of dynamic analysis, known as fuzz testing, induces program failures by deliberately introducing malformed or random data into software programs. Fuzz testing strategies derive from the intended use of applications and the associated functional and design specifications for the applications. To understand the scope of dynamic code analysis and hence the assurance provided, organizations may also consider conducting code coverage analysis (checking the degree to which the code has been tested using metrics such as percent of subroutines tested or percent of program statements called during

execution of the test suite) and/or concordance analysis (checking for words that are out of place in software code such as non-English language words or derogatory terms).
None

References

ISO/IEC 15408
NIST Special Publication 800-30
NIST Special Publication 800-53A

SUPPLY CHAIN RISK MANAGEMENT

organization-defined supply chain safeguards
organization-defined supply chain safeguards

organization-defined document
organization-defined document
name: SA-12

statement

item
name: SA-12a.

Employ to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain-related events; and

item
name: SA-12b.

Document the selected and implemented supply chain safeguards in [Selection: security and privacy plans; supply chain risk management plan;].

guidance

Supply chain-related events including, for example, disruption, theft, insertion of counterfeits, insertion of malicious code, malicious development practices, improper delivery practices, and use of defective components, can adversely impact the confidentiality, integrity, or availability of information processed, stored, or transmitted by a system. Such events can also adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. Supply chain-related events may be unintentional or malicious and occur at any point during the system life cycle. Managing supply chain risks involves gaining visibility and understanding of the processes and procedures used to protect the system, system component, or system service throughout the system life cycle. This allows organizations to make appropriate acquisition decisions and to identify

appropriate mitigation strategies. A supply chain risk management plan includes, for example, an unambiguous expression of the supply chain risk tolerance for the system, acceptable supply chain risk mitigation strategies or controls, a description of and justification for supply chain protection measures taken, a process for consistently evaluating and monitoring supply chain risk, approaches for implementing and communicating the supply chain risk management plan, and associated roles and responsibilities.

ACQUISITION STRATEGIES, TOOLS, AND METHODS

organization-defined acquisition strategies, contract tools, and procurement methods
organization-defined acquisition strategies, contract tools, and procurement methods
name: SA-12 (1)

statement

Employ to protect against, identify, and mitigate supply chain risks.

guidance

The use of the acquisition process early in the system development life cycle provides an important vehicle to protect the supply chain. There are many useful tools and techniques available including, for example, obscuring the end use of a system or system component, using blind or filtered buys, requiring tamper-evident packaging, or using trusted or controlled distribution. The results from a supply chain risk assessment can inform which strategies, tools, and methods are most applicable to the situation. Tools and techniques may provide protections against the insertion of counterfeits, tampering, theft, unauthorized production, insertion of malicious software, as well as poor manufacturing and development practices throughout the system development life cycle. Organizations also consider creating incentives for suppliers who implement security and privacy controls; promote transparency into their organizational processes and security and privacy practices; provide additional vetting of the processes and practices of subordinate suppliers, critical system components, and services; restrict purchases from specific suppliers; and provide contract language that addresses the prohibition of tainted or counterfeit components. Finally, organizations consider providing training, education, and awareness programs for organizational personnel regarding supply chain risk, available mitigation strategies, and when they should be used. Methods for reviewing and protecting development plans, evidence, and documentation are commensurate with the security category or classification level of the information system. Contracts may specify documentation protection requirements.

None

SUPPLIER REVIEWS

organization-defined frequency
organization-defined frequency
name: SA-12 (2)

statement

Review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide .

guidance

A review of supplier risk may include, for example, the ability of the supplier to effectively assess or vet any subordinate second-tier and third-tier suppliers and contractors. These reviews may be conducted by the organization or by an independent third party. The reviews consider documented processes, documented controls, publicly available information related to the supplier or contractor, and all-source intelligence where possible. The organization can use open-source information to monitor for indications of stolen CUI, poor development and quality control practices, information spillage, or counterfeits. In some cases, it may be appropriate to share review results with other organizations in accordance with any applicable inter-organizational agreements or contracts.
None

TRUSTED SHIPPING AND WAREHOUSING

name: SA-12 (3)
SA-12(1)

statement

Incorporated into SA-12(1).

DIVERSITY OF SUPPLIERS

name: SA-12 (4)
SA-12(13)

statement

Incorporated into SA-12(13).

LIMITATION OF HARM

organization-defined safeguards
organization-defined safeguards
name: SA-12 (5)

statement

Employ to limit harm from potential adversaries identifying and targeting the organizational supply chain.

guidance

Safeguards that can be implemented to reduce the probability of adversaries successfully identifying and targeting the supply chain include, for example, avoiding the purchase of custom

or non-standardized configurations; employing a diverse set of suppliers; employing approved vendor lists with standing reputations in industry; using procurement carve outs that provide exclusions to commitments or obligations; and designing the system to include diversity of materials, components, and paths. In addition, organizations consider minimizing the time between purchase decisions and required delivery to limit the opportunities for adversaries to corrupt system components.
None

MINIMIZING PROCUREMENT TIME

name: SA-12 (6)
SA-12(1)

statement

Incorporated into SA-12(1).

ASSESSMENTS PRIOR TO SELECTION, ACCEPTANCE, AND UPDATE

name: SA-12 (7)

statement

Assess the system, system component, or system service prior to selection, acceptance, modification, or update.

guidance

Organizational personnel or independent, external entities conduct assessments of systems, components, products, tools, and services to uncover unintentional and intentional vulnerabilities, evidence of tampering, or evidence of non-compliance with supply chain controls. These include, for example, malicious code, malicious processes, defective software, and counterfeits. Assessments can include, for example, visual or physical inspection; evaluations; design proposal reviews; static and dynamic analyses; visual, x-ray, or magnetic particle inspections; simulations; white, gray, and black box testing; fuzz testing; stress testing; and penetration testing. Organizations can also ensure that the components or services are genuine by using, for example, tags, cryptographic hash verifications, or digital signatures. Evidence generated during security assessments is documented for follow-on actions carried out by organizations.

USE OF ALL-SOURCE INTELLIGENCE

name: SA-12 (8)

statement

Use all-source intelligence to assist in the analysis of supply chain risk.

guidance

Organizations employ all-source intelligence to inform engineering, acquisition, and supply chain risk management decisions. All-source intelligence consists of information derived from all available sources, including, for example, publicly available or open-source information; human intelligence; signals intelligence; imagery intelligence; and measurement and signature intelligence. This information is used to analyze the risk of intentional and unintentional vulnerabilities from development, manufacturing, and delivery processes, people, and the environment. This review may be performed on suppliers at multiple tiers in the supply chain sufficient to manage risks. Organizations may develop agreements to share all-source intelligence information or resulting decisions with other organizations, as appropriate.
None

OPERATIONS SECURITY

organization-defined Operations Security (OPSEC) safeguards
organization-defined Operations Security (OPSEC) safeguards
name: SA-12 (9)

statement

Employ to protect supply chain-related information for the system, system component, or system service.

guidance

Supply chain information includes, for example, user identities; uses for systems, system components, and system services; supplier identities; supplier processes; security requirements; design specifications; testing and evaluation results; and system and component configurations. This control enhancement expands the scope of OPSEC to include suppliers and potential suppliers. OPSEC is a process of identifying critical information and subsequently analyzing friendly actions attendant to operations and other activities to identify those actions that can be observed by potential adversaries; determine indicators that potential adversaries might obtain that could be interpreted or pieced together to derive information in sufficient time to cause harm to organizations; implement safeguards or countermeasures to eliminate or reduce to an acceptable level, exploitable vulnerabilities; and finally, consider how aggregated information may compromise the confidentiality of users or the specific uses of the supply chain. OPSEC may require organizations to withhold specific mission/business information from suppliers and may include the use of intermediaries to hide the end use, or users of systems, system components, or system services.

VALIDATE AS GENUINE AND NOT ALTERED

organization-defined security safeguards
organization-defined security safeguards
name: SA-12 (10)

statement

Employ to validate that the system or system component received is genuine and has not been altered.

guidance

For many systems and system components, especially hardware, there are technical means to determine if the items are genuine or have been altered, including, for example, optical and nanotechnology tagging; physically unclonable functions; side-channel analysis; and visible anti-tamper stickers and labels. Safeguards can also include monitoring for out of specification performance, which can be an indicator of tampering or counterfeits. Suppliers and contractors may have processes for validating that a system or component is genuine and has not been altered, and for replacing a suspect system or component, which the organization may leverage. Some indications of tampering may be visible and addressable before accepting delivery including, for example, broken seals, inconsistent packaging, and incorrect labels. The organization may consider providing training to appropriate personnel on how to identify suspicious system or component deliveries. When a system or component is suspected of being altered or counterfeit, the organization considers notifying the supplier, contractor, or original equipment manufacturer who may be able to replace the item or provide a forensic capability to determine the origin of the counterfeit or altered item.

PENETRATION TESTING AND ANALYSIS

organization-defined supply chain elements, processes, and actors
organization-defined supply chain elements, processes, and actors
name: SA-12 (11)

statement

Employ [Selection (one or more): organizational analysis, independent third-party analysis, organizational penetration testing, independent third-party penetration testing] of associated with the system, system component, or system service.

guidance

This control enhancement addresses analysis or testing of the supply chain. It also considers the relationships or linkages between entities and procedures within the supply chain including, for example, development and delivery. Supply chain elements include system components that contain programmable logic and that are critically important to system functions. Supply chain processes include, for example, hardware, software, and firmware development processes; shipping and handling procedures; personnel and physical security programs; configuration management tools, techniques, and measures to maintain provenance; and programs, processes, or procedures associated with the production and distribution of supply chain elements. Supply chain actors are individuals with specific roles and responsibilities in the supply chain. The evidence generated and collected during analyses and testing of supply chain elements,

processes, and actors is documented and used to inform organizational risk management activities and decisions.

NOTIFICATION AGREEMENTS

organization-defined information
organization-defined information
name: SA-12 (12)

statement

Establish agreements and procedures with entities involved in the supply chain for the system, system component, or system service for the [Selection (one or more): notification of supply chain compromises; results of assessments or audits;].

guidance

The establishment of agreements and procedures provides for formal communications among supply chain entities. Early notification of compromises in the supply chain that can potentially adversely affect or have adversely affected organizational systems, including critical system components, is essential for organizations to effectively respond to such incidents. The results of assessments or audits may include open-source information that contributed to a decision or result and could be used to help the supply chain entity resolve a concern or improve its processes.

CRITICAL SYSTEM COMPONENTS

name: SA-12 (13)

statement

Incorporated into MA-6 and RA-9.

IDENTITY AND TRACEABILITY

organization-defined supply chain elements, processes, and personnel
organization-defined supply chain elements, processes, and personnel

organization-defined system, critical system components
organization-defined system, critical system components
name: SA-12 (14)

statement

Establish and maintain unique identification of associated with the .

guidance

Knowing who and what is in the supply chains of organizations is critical to gaining visibility into what is happening within such supply chains. It is also important for monitoring and

identifying high-risk events and activities. Without reasonable visibility and traceability into supply chains (i.e., elements, processes, and personnel), it is very difficult for organizations to understand, and therefore manage risk, and ultimately reduce the likelihood of or susceptibility to adverse events. Supply chain elements are systems or system components that contain programmable logic and that are critically important to system functions. Supply chain processes include, for example, hardware, software, and firmware development processes; shipping and handling procedures; personnel and physical security programs; configuration management tools, techniques, and measures to maintain provenance; or other programs, processes, or procedures associated with the production and distribution of supply chain elements. Supply chain personnel are individuals in the supply chain with specific roles and responsibilities related to, for example, the secure development, delivery, maintenance, and disposal of a system or system component. Tracking the unique identifiers of supply chain elements, processes, and personnel establishes a foundational identity structure for assessment of supply chain activities and for the establishment and maintenance of provenance. For example, supply chain elements may be labeled using serial numbers or tagged using radio-frequency identification tags. These labels and tags can help provide the organization better visibility into the provenance of that element. Identification methods are sufficient to support a forensic investigation in the event of a supply chain compromise or event.

PROCESSES TO ADDRESS WEAKNESSES OR DEFICIENCIES

organization-defined supply chain personnel
organization-defined supply chain personnel
name: SA-12 (15)

statement

Establish a process or processes to address weaknesses or deficiencies in supply chain elements in coordination with .

guidance

Supply chain elements are system or system components that contain programmable logic and that are critically important to system functions. Supply chain processes include, for example, hardware, software, and firmware development processes; shipping and handling procedures; personnel and physical security programs; configuration management tools, techniques, and measures to maintain provenance; or other programs, processes, or procedures associated with the production and distribution of supply chain elements. Supply chain personnel are individuals with specific roles and responsibilities in the supply chain. The evidence generated during the independent or organizational assessments of designated supply chain elements may be used to improve the supply chain processes and inform the organization#s supply chain risk management process. The evidence can also be leveraged in follow-on assessments. Evidence and other related documentation may be shared in accordance with organizational agreements.
None

PROVENANCE

organization-defined systems, system components, and associated data
organization-defined systems, system components, and associated data
name: SA-12 (16)

statement

Document, monitor, and maintain valid provenance of .

guidance

Every system and system component has a point of origin and may be changed throughout its existence. Provenance is the chronology of the origin, development, ownership, location, and changes to a system or system component and associated data. It may also include personnel and processes used to interact with or make modifications to the system, component, or associated data. Organizations consider developing procedures for allocating responsibilities for the creation, maintenance, and monitoring of provenance for systems and components; transferring provenance documentation and responsibility between organizations; and preventing and monitoring for unauthorized changes to the provenance records. Organizations consider developing methods to document, monitor, and maintain valid provenance baselines for systems, system components, and related data. Such actions help track, assess, and document changes to the provenance, including changes in supply chain elements or configuration, and ensure non-repudiation of provenance information and the provenance change records.

References

FIPS Publication 140-2
NIST Special Publication 800-30
NIST Special Publication 800-161
NIST Interagency Report 7622

TRUSTWORTHINESS

name: SA-13

statement

Incorporated into SA-8.

CRITICALITY ANALYSIS

name: SA-14

statement

Incorporated into RA-9.

DEVELOPMENT PROCESS, STANDARDS, AND TOOLS

organization-defined frequency
organization-defined frequency

organization-defined security and privacy requirements
organization-defined security and privacy requirements
name: SA-15

statement

item
name: SA-15a.

Require the developer of the system, system component, or system service to follow a documented development process that:

item
name: SA-15a.1.

Explicitly addresses security requirements;

item
name: SA-15a.2.

Identifies the standards and tools used in the development process;

item
name: SA-15a.3.

Documents the specific tool options and tool configurations used in the development process; and

item
name: SA-15a.4.

Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and

item
name: SA-15b.

Review the development process, standards, tools, tool options, and tool configurations to determine if the process, standards, tools, tool options and tool configurations selected and employed can satisfy .

guidance

Development tools include, for example, programming languages and computer-aided design systems. Reviews of development processes can include, for example, the use of maturity models to determine the potential effectiveness of such processes. Maintaining the integrity of changes to tools and processes facilitates effective supply chain risk assessment and mitigation. Such integrity requires configuration control throughout the system development life cycle to track authorized changes and to prevent unauthorized changes.

QUALITY METRICS

organization-defined frequency
organization-defined frequency

organization-defined program review milestones
organization-defined program review milestones
name: SA-15 (1)

statement

Require the developer of the system, system component, or system service to:

item
name: SA-15 (1)(a)

Define quality metrics at the beginning of the development process; and

item
name: SA-15 (1)(b)

Provide evidence of meeting the quality metrics [Selection (one or more): ; ; upon delivery].

guidance

Organizations use quality metrics to establish acceptable levels of system quality. Metrics may include quality gates which are collections of completion criteria or sufficiency standards representing the satisfactory execution of specific phases of the system development project. A quality gate, for example, may require the elimination of all compiler warnings or a determination that such warnings have no impact on the effectiveness of required security or privacy capabilities. During the execution phases of development projects, quality gates provide clear, unambiguous indications of progress. Other metrics apply to the entire development project. These metrics can include defining the severity thresholds of vulnerabilities, for example, requiring no known vulnerabilities in the delivered system with a Common Vulnerability Scoring System (CVSS) severity of Medium or High.
None

SECURITY TRACKING TOOLS
name: SA-15 (2)

statement

Require the developer of the system, system component, or system service to select and employ a security tracking tool for use during the development process.

guidance

System development teams select and deploy security tracking tools, including, for example, vulnerability/work item tracking systems that facilitate assignment, sorting, filtering, and tracking of completed work items or tasks associated with system development processes.

CRITICALITY ANALYSIS

organization-defined breadth/depth
organization-defined breadth/depth

organization-defined decision points in the system development life cycle
organization-defined decision points in the system development life cycle
name: SA-15 (3)

statement

Require the developer of the system, system component, or system service to perform a criticality analysis at and at .

guidance

This control enhancement provides developer input to the criticality analysis performed by organizations. Developer input is essential to such analysis because organizations may not have access to detailed design documentation for system components that are developed as commercial off-the-shelf products. Such design documentation includes, for example, functional specifications, high-level designs, low-level designs, and source code and hardware schematics. Criticality analysis is important for organizational systems that are designated as high value assets. Such assets can be moderate- or high-impact systems due to the potential for serious, severe, or catastrophic adverse impacts on organizational missions or business functions.

THREAT MODELING AND VULNERABILITY ANALYSIS

name: SA-15 (4)
SA-11(2)

statement

Incorporated into SA-11(2).

ATTACK SURFACE REDUCTION

organization-defined thresholds
organization-defined thresholds
name: SA-15 (5)

statement

Require the developer of the system, system component, or system service to reduce attack surfaces to .

guidance

Attack surface reduction is closely aligned with developer threat and vulnerability analyses and system architecture and design. Attack surface reduction is a means of reducing risk to organizations by giving attackers less opportunity to exploit weaknesses or deficiencies (i.e., potential vulnerabilities) within systems, system components, and system services. Attack surface reduction includes, for example, employing the concept of layered defenses; applying the principles of least privilege and least functionality; deprecating unsafe functions; applying secure software development practices including, for example, reducing the amount of code executing and reducing entry points available to unauthorized users; and eliminating application programming interfaces (APIs) that are vulnerable to attacks.

CONTINUOUS IMPROVEMENT

name: SA-15 (6)

statement

Require the developer of the system, system component, or system service to implement an explicit process to continuously improve the development process.

guidance

Developers of systems, system components, and system services consider the effectiveness and efficiency of their current development processes for meeting quality objectives and for addressing the security and privacy capabilities in current threat environments.
None

AUTOMATED VULNERABILITY ANALYSIS

organization-defined tools
organization-defined tools

organization-defined personnel or roles
organization-defined personnel or roles

name: SA-15 (7)

statement

Require the developer of the system, system component, or system service to:

item

name: SA-15 (7)(a)

Perform an automated vulnerability analysis using ;

item
name: SA-15 (7)(b)

Determine the exploitation potential for discovered vulnerabilities;

item
name: SA-15 (7)(c)

Determine potential risk mitigations for delivered vulnerabilities; and

item
name: SA-15 (7)(d)

Deliver the outputs of the tools and results of the analysis to .

guidance

None.

REUSE OF THREAT AND VULNERABILITY INFORMATION

name: SA-15 (8)

statement

Require the developer of the system, system component, or system service to use threat modeling and vulnerability analyses from similar systems, components, or services to inform the current development process.

guidance

Analysis of vulnerabilities found in similar software applications can inform potential design and implementation issues for systems under development. Similar systems or system components may exist within developer organizations. Vulnerability information is available from a variety of public and private sector sources including, for example, the NIST National Vulnerability Database.
None

USE OF LIVE DATA

name: SA-15 (9)
SA-3(2)

statement

Incorporated into SA-3(2).

INCIDENT RESPONSE PLAN

name: SA-15 (10)

statement

Require the developer of the system, system component, or system service to provide, implement, and test an incident response plan.

guidance

The incident response plan provided by developers of systems, system components, and system services may be incorporated into organizational incident response plans. This information provides the type of incident response information that is not readily available to organizations. Such information may be extremely helpful, for example, when organizations respond to vulnerabilities in commercial off-the-shelf products.

ARCHIVE SYSTEM OR COMPONENT

name: SA-15 (11)

statement

Require the developer of the system or system component to archive the system or component to be released or delivered together with the corresponding evidence supporting the final security and privacy review.

guidance

Archiving system or system components requires the developer to retain key development artifacts including, for example, hardware specifications, source code, object code, and any relevant documentation from the development process that can provide a readily available configuration baseline for system and component upgrades or modifications.
None

DEVELOPER-PROVIDED TRAINING

organization-defined training
organization-defined training
name: SA-16

statement

Require the developer of the system, system component, or system service to provide on the correct use and operation of the implemented security and privacy functions, controls, and/or mechanisms.

guidance

This control applies to external and internal (in-house) developers. Training of personnel is an essential element to ensure the effectiveness of the security and privacy controls implemented within organizational systems. Training options include, for example, web-based and computer-based training; classroom-style training; and hands-on training. Organizations can also request

training materials from developers to conduct in-house training or offer self-training to organizational personnel. Organizations determine the type of training necessary and may require different types of training for different security and privacy functions, controls, and mechanisms.

DEVELOPER SECURITY ARCHITECTURE AND DESIGN

name: SA-17

statement

Require the developer of the system, system component, or system service to produce a design specification and security architecture that:

item

name: SA-17a.

Is consistent with and supportive of the organization#s security architecture which is established within and is an integrated part of the organization#s enterprise architecture;

item

name: SA-17b.

Accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components; and

item

name: SA-17c.

Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection.

guidance

This control is primarily directed at external developers, although it could also be used for internal (in-house) development. In contrast, PL-8 is primarily directed at internal developers to ensure that organizations develop a security architecture and that the architecture is integrated or tightly coupled to the enterprise architecture. This distinction is important when organizations outsource the development of systems, system components, or system services to external entities, and when there is a requirement to demonstrate consistency with the enterprise architecture and security architecture of the organization. ISO/IEC 15408 provides additional information on security architecture and design including, for example, formal policy models, security-relevant components, formal and informal correspondence, conceptually simple design, and structuring for least privilege and testing.

FORMAL POLICY MODEL

organization-defined elements of organizational security policy
organization-defined elements of organizational security policy

name: SA-17 (1)

statement

Require the developer of the system, system component, or system service to:

item
name: SA-17 (1)(a)

Produce, as an integral part of the development process, a formal policy model describing the to be enforced; and

item
name: SA-17 (1)(b)

Prove that the formal policy model is internally consistent and sufficient to enforce the defined elements of the organizational security policy when implemented.

guidance

Formal models describe specific behaviors or security policies using formal languages, thus enabling the correctness of those behaviors and policies to be formally proven. Not all components of systems can be modeled. Generally, formal specifications are scoped to the specific behaviors or policies of interest, for example, nondiscretionary access control policies. Organizations choose the formal modeling language and approach based on the nature of the behaviors and policies to be described and the available tools. Examples of formal modeling tools include Gypsy and Zed.
None

SECURITY-RELEVANT COMPONENTS

name: SA-17 (2)

statement

Require the developer of the system, system component, or system service to:

item
name: SA-17 (2)(a)

Define security-relevant hardware, software, and firmware; and

item
name: SA-17 (2)(b)

Provide a rationale that the definition for security-relevant hardware, software, and firmware is complete.

guidance

The security-relevant hardware, software, and firmware represent the portion of the system, component, or service that must be trusted to perform correctly to maintain required security properties.

FORMAL CORRESPONDENCE

name: SA-17 (3)

statement

Require the developer of the system, system component, or system service to:

item

name: SA-17 (3)(a)

Produce, as an integral part of the development process, a formal top-level specification that specifies the interfaces to security-relevant hardware, software, and firmware in terms of exceptions, error messages, and effects;

item

name: SA-17 (3)(b)

Show via proof to the extent feasible with additional informal demonstration as necessary, that the formal top-level specification is consistent with the formal policy model;

item

name: SA-17 (3)(c)

Show via informal demonstration, that the formal top-level specification completely covers the interfaces to security-relevant hardware, software, and firmware;

item

name: SA-17 (3)(d)

Show that the formal top-level specification is an accurate description of the implemented security-relevant hardware, software, and firmware; and

item

name: SA-17 (3)(e)

Describe the security-relevant hardware, software, and firmware mechanisms not addressed in the formal top-level specification but strictly internal to the security-relevant hardware, software, and firmware.

guidance

Correspondence is an important part of the assurance gained through modeling. It demonstrates that the implementation is an accurate transformation of the model, and that any additional code or implementation details that are present have no impact on the behaviors or policies being modeled. Formal methods can be used to show that the high-level security properties are

satisfied by the formal system description, and that the formal system description is correctly implemented by a description of some lower level, for example a hardware description. Consistency between the formal top-level specification and the formal policy models is generally not amenable to being fully proven. Therefore, a combination of formal and informal methods may be needed to show such consistency. Consistency between the formal top-level specification and the actual implementation may require the use of an informal demonstration due to limitations in the applicability of formal methods to prove that the specification accurately reflects the implementation. Hardware, software, and firmware mechanisms strictly internal to security-relevant hardware, software, and firmware include, for example, mapping registers and direct memory input and output.

INFORMAL CORRESPONDENCE

name: SA-17 (4)

statement

Require the developer of the system, system component, or system service to:

item

name: SA-17 (4)(a)

Produce, as an integral part of the development process, an informal descriptive top-level specification that specifies the interfaces to security-relevant hardware, software, and firmware in terms of exceptions, error messages, and effects;

item

name: SA-17 (4)(b)

Show via [Selection: informal demonstration, convincing argument with formal methods as feasible] that the descriptive top-level specification is consistent with the formal policy model;

item

name: SA-17 (4)(c)

Show via informal demonstration, that the descriptive top-level specification completely covers the interfaces to security-relevant hardware, software, and firmware;

item

name: SA-17 (4)(d)

Show that the descriptive top-level specification is an accurate description of the interfaces to security-relevant hardware, software, and firmware; and

item

name: SA-17 (4)(e)

Describe the security-relevant hardware, software, and firmware mechanisms not addressed in the descriptive top-level specification but strictly internal to the security-relevant hardware, software, and firmware.

guidance

Correspondence is an important part of the assurance gained through modeling. It demonstrates that the implementation is an accurate transformation of the model, and that any additional code or implementation details present has no impact on the behaviors or policies being modeled. Consistency between the descriptive top-level specification (i.e., high-level/low-level design) and the formal policy model is generally not amenable to being fully proven. Therefore, a combination of formal and informal methods may be needed to show such consistency. Hardware, software, and firmware mechanisms strictly internal to security-relevant hardware, software, and firmware include, for example, mapping registers and direct memory input and output.

CONCEPTUALLY SIMPLE DESIGN

name: SA-17 (5)

statement

Require the developer of the system, system component, or system service to:

item
name: SA-17 (5)(a)

Design and structure the security-relevant hardware, software, and firmware to use a complete, conceptually simple protection mechanism with precisely defined semantics; and

item
name: SA-17 (5)(b)

Internally structure the security-relevant hardware, software, and firmware with specific regard for this mechanism.

guidance

None.

STRUCTURE FOR TESTING

name: SA-17 (6)

statement

Require the developer of the system, system component, or system service to structure security-relevant hardware, software, and firmware to facilitate testing.

guidance

None.

STRUCTURE FOR LEAST PRIVILEGE

name: SA-17 (7)

statement

Require the developer of the system, system component, or system service to structure security-relevant hardware, software, and firmware to facilitate controlling access with least privilege.

guidance

None.

References

ISO/IEC 15408

TAMPER RESISTANCE AND DETECTION

name: SA-18

statement

Implement a tamper protection program for the system, system component, or system service.

guidance

Anti-tamper technologies, tools, and techniques provide a level of protection for systems and system components against many threats including reverse engineering, modification, and substitution. Strong identification combined with tamper resistance and/or tamper detection is essential to protecting systems and components during distribution and when in use.

MULTIPLE PHASES OF SYSTEM DEVELOPMENT LIFE CYCLE

name: SA-18 (1)

statement

Employ anti-tamper technologies, tools, and techniques during multiple phases in the system development life cycle including design, development, integration, operations, and maintenance.

guidance

Organizations use a combination of hardware and software techniques for tamper resistance and detection. Organizations employ obfuscation and self-checking, for example, to make reverse engineering and modifications more difficult, time-consuming, and expensive for adversaries. The customization of systems and system components can make substitutions easier to detect and therefore limit damage.

INSPECTION OF SYSTEMS OR COMPONENTS

organization-defined systems or system components
organization-defined systems or system components

organization-defined frequency
organization-defined frequency

organization-defined indications of need for inspection
organization-defined indications of need for inspection
name: SA-18 (2)

statement

Inspect [Selection (one or more): at random; at , upon] to detect tampering.

guidance

This control enhancement addresses physical and logical tampering and is typically applied to mobile devices, notebook computers, or other system components taken out of organization-controlled areas. Indications of a need for inspection include, for example, when individuals return from travel to high-risk locations.

COMPONENT AUTHENTICITY

organization-defined external reporting organizations
organization-defined external reporting organizations

organization-defined personnel or roles
organization-defined personnel or roles
name: SA-19

statement

item
name: SA-19a.

Develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system; and

item
name: SA-19b.

Report counterfeit system components to [Selection (one or more): source of counterfeit component; ;].

guidance

Sources of counterfeit components include, for example, manufacturers, developers, vendors, and contractors. Anti-counterfeiting policy and procedures support tamper resistance and provide a level of protection against the introduction of malicious code. External reporting organizations include, for example, US-CERT.

ANTI-COUNTERFEIT TRAINING

organization-defined personnel or roles
organization-defined personnel or roles
name: SA-19 (1)

statement

Train to detect counterfeit system components (including hardware, software, and firmware).

guidance

None.

CONFIGURATION CONTROL FOR COMPONENT SERVICE AND REPAIR

organization-defined system components
organization-defined system components
name: SA-19 (2)

statement

Maintain configuration control over awaiting service or repair and serviced or repaired components awaiting return to service.

guidance

None.

COMPONENT DISPOSAL

organization-defined techniques and methods
organization-defined techniques and methods
name: SA-19 (3)

statement

Dispose of system components using .

guidance

Proper disposal of system components helps to prevent such components from entering the gray market.

ANTI-COUNTERFEIT SCANNING

organization-defined frequency
organization-defined frequency
name: SA-19 (4)

statement

Scan for counterfeit system components .

guidance

None.

CUSTOMIZED DEVELOPMENT OF CRITICAL COMPONENTS

organization-defined critical system components
organization-defined critical system components
name: SA-20

statement

Re-implement or custom develops .

guidance

Organizations determine that certain system components likely cannot be trusted due to specific threats to and vulnerabilities in those components, and for which there are no viable security controls to adequately mitigate the resulting risk. Re-implementation or custom development of such components helps to satisfy requirements for higher assurance. This is accomplished by initiating changes to system components (including hardware, software, and firmware) such that the standard attacks by adversaries are less likely to succeed. In situations where no alternative sourcing is available and organizations choose not to re-implement or custom develop critical system components, additional safeguards can be employed. These include, for example, enhanced auditing; restrictions on source code and system utility access; and protection from deletion of system and application files.

DEVELOPER SCREENING

organization-defined system, system component, or system service
organization-defined system, system component, or system service

organization-defined official government duties
organization-defined official government duties

organization-defined additional personnel screening criteria
organization-defined additional personnel screening criteria
name: SA-21

statement

Require that the developer of :

item
name: SA-21a.

Have appropriate access authorizations as determined by assigned ;

item
name: SA-21b.

Satisfy ; and

item
name: SA-21c.

Provide information that the access authorizations and screening criteria specified in a. and b. are satisfied.

guidance

This control is directed at external developers. Because the system, system component, or system service may be employed in critical activities essential to the national or economic security interests of the United States, organizations have a strong interest in ensuring that the developer is trustworthy. The degree of trust required of the developer may need to be consistent with that of the individuals accessing the system/component/service once deployed. Examples of authorization and personnel screening criteria include clearances, background checks, citizenship, and nationality. Trustworthiness of developers may also include a review and analysis of company ownership and any relationships the company has with entities potentially affecting the quality and reliability of the systems, components, or services being developed. Satisfying required access authorizations and personnel screening criteria includes, for example, providing a list of all individuals who are authorized to perform development activities on the selected system, system component, or system service so that organizations can validate that the developer has satisfied the authorization and screening requirements.

VALIDATION OF SCREENING

name: SA-21 (1)

statement

Incorporated into SA-21.

UNSUPPORTED SYSTEM COMPONENTS

name: SA-22

statement

Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer.

guidance

Support for system components includes, for example, software patches, firmware updates, replacement parts, and maintenance contracts. Unsupported components, for example, when vendors no longer provide critical software patches or product updates, provide an opportunity for adversaries to exploit weaknesses in the installed components. Exceptions to replacing unsupported system components may include, for example, systems that provide critical mission or business capability where newer technologies are not available or where the systems are so isolated that installing replacement components is not an option.

ALTERNATIVE SOURCES FOR CONTINUED SUPPORT

organization-defined support from external providers
organization-defined support from external providers

name: SA-22 (1)

statement

Provide [Selection (one or more): in-house support;] for unsupported system components.

guidance

This control enhancement addresses the need to provide continued support for system components that are no longer supported by the original manufacturers, developers, or vendors when such components remain essential to organizational mission and business operations. Organizations can establish in-house support, for example, by developing customized patches for critical software components or alternatively, obtain the services of external providers who through contractual relationships, provide ongoing support for the designated unsupported components. Such contractual relationships can include, for example, Open Source Software value-added vendors.
None

SYSTEM AND COMMUNICATIONS PROTECTION

SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES

organization-defined personnel or roles
organization-defined personnel or roles

organization-defined senior management official
organization-defined senior management official

organization-defined frequency
organization-defined frequency

organization-defined frequency
organization-defined frequency
name: SC-1

statement

item
name: SC-1a.

Develop, document, and disseminate to :

item
name: SC-1a.1.

A system and communications protection policy that:

item
name: SC-1a.1.(a)

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

item
name: SC-1a.1.(b)

Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and

item
name: SC-1a.2.

Procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection controls;

item
name: SC-1b.

Designate an to manage the system and communications protection policy and procedures;

item
name: SC-1c.

Review and update the current system and communications protection:

item
name: SC-1c.1.

Policy ; and

item
name: SC-1c.2.

Procedures ;

item
name: SC-1d.

Ensure that the system and communications protection procedures implement the system and communications protection policy and controls; and

item
name: SC-1e.

Develop, document, and implement remediation actions for violations of the system and communications protection policy.

guidance

This control addresses the establishment of policy and procedures for the effective implementation of the controls and control enhancements in the SC family. The risk management strategy is an important factor in establishing policy and procedures. Comprehensive policy and procedures help provide security and privacy assurance. Security and privacy program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general security and privacy policy or can be represented by multiple policies reflecting the complex nature of organizations. The procedures can be established for security and privacy programs and for systems, if needed. Procedures describe how policies or controls are implemented and can be directed at the personnel or role that is the object of the procedure. Procedures can be documented in system security and plans or in one or more separate documents. It is important to recognize that restating controls does not constitute an organizational policy or procedure.

References

NIST Special Publication 800-12
NIST Special Publication 800-100

APPLICATION PARTITIONING
name: SC-2

statement

Separate user functionality, including user interface services, from system management functionality.

guidance

System management functionality includes, for example, functions that are necessary to administer databases, network components, workstations, or servers. These functions typically require privileged user access. The separation of user functions from system management functions is either physical or logical. Organizations implement separation of system management functions from user functions, for example, by using different computers, instances of operating systems, central processing units, or network addresses; by employing virtualization techniques; or some combination of these or other methods. This type of separation includes, for example, web administrative interfaces that use separate authentication methods for users of any other system resources. Separation of system and user functions may include isolating administrative interfaces on different domains and with additional access controls.

INTERFACES FOR NON-PRIVILEGED USERS
name: SC-2 (1)

statement

Prevent the presentation of system management functionality at an interface for non-privileged users.

guidance

This control enhancement ensures that system administration options including administrator privileges, are not available to general users. This type of restricted access also prohibits the use of the grey-out option commonly used to eliminate accessibility to such information. One potential solution is to withhold administration options until users establish sessions with administrator privileges.

SECURITY FUNCTION ISOLATION
name: SC-3

statement

Isolate security functions from nonsecurity functions.

guidance

The system isolates security functions from nonsecurity functions by means of an isolation boundary implemented via partitions and domains. Such isolation controls access to and protects the integrity of the hardware, software, and firmware that perform those security functions. Systems implement code separation in many ways, for example, through the provision of security kernels via processor rings or processor modes. For non-kernel code, security function isolation is often achieved through file system protections that protect the code on disk and address space protections that protect executing code. Systems can restrict access to security functions using access control mechanisms and by implementing least privilege capabilities. While the ideal is for all code within the defined security function isolation boundary to only contain security-relevant code, it is sometimes necessary to include nonsecurity functions within the isolation boundary as an exception.

HARDWARE SEPARATION

name: SC-3 (1)

statement

Use hardware separation mechanisms to implement security function isolation.

guidance

Hardware separation mechanisms include, for example, hardware ring architectures that are commonly implemented within microprocessors, and hardware-enforced address segmentation used to support logically distinct storage objects with separate attributes (i.e., readable, writeable).

None

ACCESS AND FLOW CONTROL FUNCTIONS

name: SC-3 (2)

statement

Isolate security functions enforcing access and information flow control from nonsecurity functions and from other security functions.

guidance

Security function isolation occurs because of implementation. The functions can still be scanned and monitored. Security functions that are potentially isolated from access and flow control enforcement functions include, for example, auditing, intrusion detection, and anti-virus functions.

None

MINIMIZE NONSECURITY FUNCTIONALITY

name: SC-3 (3)

statement

Minimize the number of nonsecurity functions included within the isolation boundary containing security functions.

guidance

In those instances where it is not feasible to achieve strict isolation of nonsecurity functions from security functions, it is necessary to take actions to minimize the nonsecurity-relevant functions within the security function boundary. Nonsecurity functions contained within the isolation boundary are considered security-relevant because errors or the maliciousness in such software, can directly impact the security functions of systems. The fundamental design objective is that the specific portions of systems providing information security are of minimal size and complexity. Minimizing the number of nonsecurity functions in the security-relevant system components allows designers and implementers to focus only on those functions which are necessary to provide the desired security capability (typically access enforcement). By minimizing nonsecurity functions within the isolation boundaries, the amount of code that must be trusted to enforce security policies is significantly reduced, thus contributing to understandability.

None

MODULE COUPLING AND COHESIVENESS

name: SC-3 (4)

statement

Implement security functions as largely independent modules that maximize internal cohesiveness within modules and minimize coupling between modules.

guidance

The reduction in inter-module interactions helps to constrain security functions and to manage complexity. The concepts of coupling and cohesion are important with respect to modularity in software design. Coupling refers to the dependencies that one module has on other modules. Cohesion refers to the relationship between different functions within a module. Best practices in software engineering rely on layering, minimization, and modular decomposition to reduce and manage complexity. This produces software modules that are highly cohesive and loosely coupled.

None

LAYERED STRUCTURES

name: SC-3 (5)

statement

Implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.

guidance

The implementation of layered structures with minimized interactions among security functions and non-looping layers (i.e., lower-layer functions do not depend on higher-layer functions) further enables the isolation of security functions and management of complexity.
None

INFORMATION IN SHARED SYSTEM RESOURCES
name: SC-4

statement

Prevent unauthorized and unintended information transfer via shared system resources.

guidance

This control prevents information produced by the actions of prior users or roles (or the actions of processes acting on behalf of prior users or roles) from being available to current users or roles (or current processes acting on behalf of current users or roles) that obtain access to shared system resources after those resources have been released back to the system. This control also applies to encrypted representations of information. The control of information in shared system resources is referred to as object reuse and residual information protection. This control does not address information remanence which refers to the residual representation of data that has been nominally deleted; covert channels (including storage and timing channels) where shared system resources are manipulated to violate information flow restrictions; or components within systems for which there are only single users or roles.

SECURITY LEVELS
name: SC-4 (1)

statement

Incorporated into SC-4.

MULTILEVEL OR PERIODS PROCESSING

organization-defined procedures
organization-defined procedures
name: SC-4 (2)

statement

Prevent unauthorized information transfer via shared resources in accordance with when system processing explicitly switches between different information classification levels or security categories.

guidance

This control enhancement applies when there are explicit changes in information processing levels during system operations. This situation can occur, for example, during multilevel or periods processing with information at different classification levels or security categories. Organization-defined procedures may include, for example, approved sanitization processes for electronically stored information.
None

DENIAL OF SERVICE PROTECTION

organization-defined types of denial of service events or references to sources for such information
organization-defined types of denial of service events or references to sources for such information

organization-defined security safeguards
organization-defined security safeguards
name: SC-5

statement

Protect against or limit the effects of the following types of denial of service events: by employing .

guidance

Denial of service may occur because of an attack by an adversary or a lack of internal planning to support organizational needs with respect to capacity and bandwidth. There are a variety of technologies available to limit or eliminate the effects of denial of service events. For example, boundary protection devices can filter certain types of packets to protect system components on internal networks from being directly affected by denial of service attacks. Employing increased network capacity and bandwidth combined with service redundancy also reduces the susceptibility to denial of service events.

RESTRICT INTERNAL USERS

organization-defined denial of service attacks
organization-defined denial of service attacks
name: SC-5 (1)

statement

Restrict the ability of individuals to launch against other systems.

guidance

Restricting the ability of individuals to launch denial of service attacks requires that the mechanisms commonly used for such attacks are unavailable. Individuals of concern can include, for example, hostile insiders or external adversaries that have breached or compromised the system and are subsequently using the system to launch attacks on other individuals or organizations. Organizations can restrict the ability of individuals to connect and transmit arbitrary information on the transport medium (i.e., wired or wireless networks). Organizations can also limit the ability of individuals to use excessive system resources. Protection against individuals having the ability to launch denial of service attacks may be implemented on specific systems or on boundary devices prohibiting egress to potential target systems.
None

CAPACITY, BANDWIDTH, AND REDUNDANCY

name: SC-5 (2)

statement

Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding denial of service attacks.

guidance

Managing capacity ensures that sufficient capacity is available to counter flooding attacks. Managing capacity may include, for example, establishing selected usage priorities, quotas, or partitioning.
None

DETECTION AND MONITORING

organization-defined monitoring tools
organization-defined monitoring tools

organization-defined system resources
organization-defined system resources

name: SC-5 (3)

statement

item

name: SC-5 (3)(a)

Employ to detect indicators of denial of service attacks against the system; and

item
name: SC-5 (3)(b)

Monitor to determine if sufficient resources exist to prevent effective denial of service attacks.

guidance

Organizations consider utilization and capacity of system resources when managing risk from denial of service due to malicious attacks. Denial of service attacks can originate from external or internal sources. System resources sensitive to denial of service include, for example, physical disk storage, memory, and CPU cycles. Examples of common safeguards used to prevent denial of service attacks related to storage utilization and capacity include, instituting disk quotas; configuring systems to automatically alert administrators when specific storage capacity thresholds are reached; using file compression technologies to maximize available storage space; and imposing separate partitions for system and user data.

RESOURCE AVAILABILITY

organization-defined resources
organization-defined resources

organization-defined security safeguards
organization-defined security safeguards
name: SC-6

statement

Protect the availability of resources by allocating by [Selection (one or more); priority; quota;].

guidance

Priority protection prevents lower-priority processes from delaying or interfering with the system servicing higher-priority processes. Quotas prevent users or processes from obtaining more than predetermined amounts of resources. This control does not apply to system components for which there are only single users or roles.

BOUNDARY PROTECTION
name: SC-7

statement

item
name: SC-7a.

Monitor and control communications at the external boundary of the system and at key internal boundaries within the system;

item
name: SC-7b.

Implement subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and

item
name: SC-7c.

Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.

guidance

Managed interfaces include, for example, gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within a security architecture. Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones or DMZs. Restricting or prohibiting interfaces within organizational systems includes, for example, restricting external web traffic to designated web servers within managed interfaces and prohibiting external traffic that appears to be spoofing internal addresses. Commercial telecommunications services are typically provided by network components and consolidated management systems shared by customers. These services may also include third party-provided access lines and other service elements. Such services may represent sources of increased risk despite contract security provisions.

PHYSICALLY SEPARATED SUBNETWORKS

name: SC-7 (1)

statement

Incorporated into SC-7.

PUBLIC ACCESS

name: SC-7 (2)

statement

Incorporated into SC-7.

ACCESS POINTS

name: SC-7 (3)

statement

Limit the number of external network connections to the system.

guidance

Limiting the number of external network connections facilitates more comprehensive monitoring of inbound and outbound communications traffic. The Trusted Internet Connection initiative is an example of limiting the number of external network connections.
None

EXTERNAL TELECOMMUNICATIONS SERVICES

organization-defined frequency
organization-defined frequency
name: SC-7 (4)

statement

item
name: SC-7 (4)(a)

Implement a managed interface for each external telecommunication service;

item
name: SC-7 (4)(b)

Establish a traffic flow policy for each managed interface;

item
name: SC-7 (4)(c)

Protect the confidentiality and integrity of the information being transmitted across each interface;

item
name: SC-7 (4)(d)

Document each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and

item
name: SC-7 (4)(e)

Review exceptions to the traffic flow policy and removes exceptions that are no longer supported by an explicit mission/business need.

guidance

None.

DENY BY DEFAULT # ALLOW BY EXCEPTION

name: SC-7 (5)

statement

Deny network communications traffic by default and allow network communications traffic by exception at managed interfaces.

guidance

This control enhancement applies to inbound and outbound network communications traffic. A deny-all, permit-by-exception network communications traffic policy ensures that only those system connections which are essential and approved are allowed. This requirement differs from CA-3(5) in that it applies to any type of network communications while CA-3(5) is applied to a system that is interconnected with another system.

RESPONSE TO RECOGNIZED FAILURES

name: SC-7 (6)
SC-7(18)

statement

Incorporated into SC-7(18).

PREVENT SPLIT TUNNELING FOR REMOTE DEVICES

name: SC-7 (7)

statement

Prevent a remote device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks.

guidance

This control enhancement is implemented in remote devices including, for example, notebook computers, through configuration settings to disable split tunneling in those devices, and by preventing those configuration settings from being readily configurable by users. This control enhancement is implemented within the system by the detection of split tunneling (or of configuration settings that allow split tunneling) in the remote device, and by prohibiting the connection if the remote device is using split tunneling. Split tunneling might be desirable by remote users to communicate with local system resources such as printers or file servers. However, split tunneling can allow unauthorized external connections, making the system more vulnerable to attack and to exfiltration of organizational information. The use of VPNs for remote connections, when adequately provisioned with the appropriate security controls, may provide the organization with sufficient assurance that it can effectively treat such connections as non-remote connections with respect to the objectives of confidentiality and integrity. VPNs provide a means for allowing non-remote communications paths from remote devices. The use of an adequately provisioned VPN does not eliminate the need for preventing split tunneling.
None

ROUTE TRAFFIC TO AUTHENTICATED PROXY SERVERS

organization-defined internal communications traffic
organization-defined internal communications traffic

organization-defined external networks
organization-defined external networks
name: SC-7 (8)

statement

Route to through authenticated proxy servers at managed interfaces.

guidance

External networks are networks outside of organizational control. A proxy server is a server (i.e., system or application) that acts as an intermediary for clients requesting system resources from non-organizational or other organizational servers. These system resources can include, for example, files, connections, web pages, or services. Client requests established through an initial connection to the proxy server are evaluated to manage complexity and to provide additional protection by limiting direct connectivity. Web content filtering devices are one of the most common proxy servers providing access to the Internet. Proxy servers can support logging of individual Transmission Control Protocol sessions and blocking specific Uniform Resource Locators, Internet Protocol addresses, and domain names. Web proxies can be configured with organization-defined lists of authorized and unauthorized websites.

RESTRICT THREATENING OUTGOING COMMUNICATIONS TRAFFIC

name: SC-7 (9)

statement

item
name: SC-7 (9)(a)

Detect and deny outgoing communications traffic posing a threat to external systems; and

item
name: SC-7 (9)(b)

Audit the identity of internal users associated with denied communications.

guidance

Detecting outgoing communications traffic from internal actions that may pose threats to external systems is known as extrusion detection. Extrusion detection is carried out at system boundaries as part of managed interfaces. This capability includes the analysis of incoming and

outgoing communications traffic while searching for indications of internal threats to the security of external systems. Such threats include, for example, traffic indicative of denial of service attacks and traffic containing malicious code.

PREVENT EXFILTRATION

organization-defined frequency
organization-defined frequency
name: SC-7 (10)

statement

item
name: SC-7 (10)(a)

Prevent the exfiltration of information; and

item
name: SC-7 (10)(b)

Conduct exfiltration tests .

guidance

This control enhancement applies to intentional and unintentional exfiltration of information. Safeguards to prevent exfiltration of information from systems may be implemented at internal endpoints, external boundaries, and across managed interfaces and include, for example, strict adherence to protocol formats; monitoring for beaconing activity from systems; monitoring for steganography; disconnecting external network interfaces except when explicitly needed; disassembling and reassembling packet headers; employing traffic profile analysis to detect deviations from the volume and types of traffic expected within organizations or call backs to command and control centers; and implementing data loss and data leakage prevention tools. Devices that enforce strict adherence to protocol formats include, for example, deep packet inspection firewalls and XML gateways. These devices verify adherence to protocol formats and specifications at the application layer and identify vulnerabilities that cannot be detected by devices operating at the network or transport layers. This control enhancement is analogous with data loss/data leakage prevention and is closely associated with cross-domain solutions and system guards enforcing information flow requirements.

RESTRICT INCOMING COMMUNICATIONS TRAFFIC

organization-defined authorized sources
organization-defined authorized sources

organization-defined authorized destinations
organization-defined authorized destinations
name: SC-7 (11)

statement

Only allow incoming communications from to be routed to .

guidance

This control enhancement provides determinations that source and destination address pairs represent authorized/allowed communications. Such determinations can be based on several factors including, for example, the presence of such address pairs in the lists of authorized/ allowed communications; the absence of such address pairs in lists of unauthorized/disallowed pairs; or meeting more general rules for authorized/allowed source and destination pairs.

HOST-BASED PROTECTION

organization-defined host-based boundary protection mechanisms
organization-defined host-based boundary protection mechanisms

organization-defined system components
organization-defined system components
name: SC-7 (12)

statement

Implement at .

guidance

Host-based boundary protection mechanisms include, for example, host-based firewalls. Examples of system components employing host-based boundary protection mechanisms include servers, workstations, notebook computers, and mobile devices.
None

ISOLATION OF SECURITY TOOLS, MECHANISMS, AND SUPPORT COMPONENTS

organization-defined information security tools, mechanisms, and support components
organization-defined information security tools, mechanisms, and support components
name: SC-7 (13)

statement

Isolate from other internal system components by implementing physically separate subnetworks with managed interfaces to other components of the system.

guidance

Physically separate subnetworks with managed interfaces are useful, for example, in isolating computer network defenses from critical operational processing networks to prevent adversaries from discovering the analysis and forensics techniques of organizations.

PROTECTS AGAINST UNAUTHORIZED PHYSICAL CONNECTIONS

organization-defined managed interfaces
organization-defined managed interfaces
name: SC-7 (14)

statement

Protect against unauthorized physical connections at .

guidance

Systems operating at different security categories or classification levels may share common physical and environmental controls, since the systems may share space within the same facilities. In practice, it is possible that these separate systems may share common equipment rooms, wiring closets, and cable distribution paths. Protection against unauthorized physical connections can be achieved, for example, by employing clearly identified and physically separated cable trays, connection frames, and patch panels for each side of managed interfaces with physical access controls enforcing limited authorized access to these items.

ROUTE PRIVILEGED NETWORK ACCESSES

name: SC-7 (15)

statement

Route all networked, privileged accesses through a dedicated, managed interface for purposes of access control and auditing.

guidance

None.

PREVENT DISCOVERY OF COMPONENTS AND DEVICES

name: SC-7 (16)

statement

Prevent the discovery of specific system components that represent a managed interface.

guidance

This control enhancement protects network addresses of system components that are part of managed interfaces from discovery through common tools and techniques used to identify devices on networks. Network addresses are not available for discovery, requiring prior

knowledge for access. This can be accomplished by not publishing network addresses or entering the addresses in domain name systems. Another obfuscation technique is to periodically change network addresses.
None

AUTOMATED ENFORCEMENT OF PROTOCOL FORMATS

name: SC-7 (17)

statement

Enforce adherence to protocol formats.

guidance

Examples of system components that enforce protocol formats include deep packet inspection firewalls and XML gateways. Such components verify adherence to protocol formats and specifications at the application layer and identify vulnerabilities that cannot be detected by devices operating at the network or transport layers.

FAIL SECURE

name: SC-7 (18)

statement

Prevent systems from entering unsecure states in the event of an operational failure of a boundary protection device.

guidance

Fail secure is a condition achieved by employing system mechanisms to ensure that in the event of operational failures of boundary protection devices at managed interfaces, systems do not enter into unsecure states where intended security properties no longer hold. Examples of managed interfaces include routers, firewalls, and application gateways residing on protected subnetworks commonly referred to as demilitarized zones. Failures of boundary protection devices cannot lead to, or cause information external to the devices to enter the devices, nor can failures permit unauthorized information releases.

BLOCK COMMUNICATION FROM NON-ORGANIZATIONALLY CONFIGURED HOSTS

organization-defined communication clients
organization-defined communication clients
name: SC-7 (19)

statement

Block inbound and outbound communications traffic between that are independently configured by end users and external service providers.

guidance

Communication clients independently configured by end users and external service providers include, for example, instant messaging clients. Traffic blocking does not apply to communication clients that are configured by organizations to perform authorized functions.
None

DYNAMIC ISOLATION AND SEGREGATION

organization-defined system components
organization-defined system components
name: SC-7 (20)

statement

Provide the capability to dynamically isolate or segregate from other system components.

guidance

The capability to dynamically isolate or segregate certain internal components of organizational systems is useful when it is necessary to partition or separate certain system components of questionable origin from those components possessing greater trustworthiness. Component isolation reduces the attack surface of organizational systems. Isolating selected system components can also limit the damage from successful attacks when such attacks occur.
None

ISOLATION OF SYSTEM COMPONENTS

organization-defined system components
organization-defined system components

organization-defined missions and/or business functions
organization-defined missions and/or business functions
name: SC-7 (21)

statement

Employ boundary protection mechanisms to separate supporting .

guidance

Organizations can isolate system components performing different missions or business functions. Such isolation limits unauthorized information flows among system components and provides the opportunity to deploy greater levels of protection for selected system components. Separating system components with boundary protection mechanisms provides the capability for increased protection of individual components and to more effectively control information flows between those components. This type of enhanced protection limits the potential harm from hostile attacks and errors. The degree of separation provided varies depending upon the

mechanisms chosen. Boundary protection mechanisms include, for example, routers, gateways, and firewalls separating system components into physically separate networks or subnetworks; cross-domain devices separating subnetworks; virtualization techniques; and encrypting information flows among system components using distinct encryption keys.

SEPARATE SUBNETS FOR CONNECTING TO DIFFERENT SECURITY DOMAINS

name: SC-7 (22)

statement

Implement separate network addresses to connect to systems in different security domains.

guidance

The decomposition of systems into subnetworks (subnets) helps to provide the appropriate level of protection for network connections to different security domains containing information with different security categories or classification levels.

None

DISABLE SENDER FEEDBACK ON PROTOCOL VALIDATION FAILURE

name: SC-7 (23)

statement

Disable feedback to senders on protocol format validation failure.

guidance

Disabling feedback to senders when there is a failure in protocol validation format prevents adversaries from obtaining information which would otherwise be unavailable.

None

PERSONALLY IDENTIFIABLE INFORMATION

organization-defined processing rules
organization-defined processing rules

name: SC-7 (24)

statement

For systems that process, store, or transmit personally identifiable information:

item

name: SC-7 (24)(a)

Apply to data elements of personally identifiable information;

item
name: SC-7 (24)(b)

Monitor for permitted processing at the external boundary of the system and at key internal boundaries within the system;

item
name: SC-7 (24)(c)

Document each processing exception; and

item
name: SC-7 (24)(d)

Review and remove exceptions that are no longer supported.

guidance

Managing the transmission of personally identifiable information and how such information is used is an important aspect of safeguarding an individual#s privacy. Processing rules that determine how or when personally identifiable information may be used or transmitted ensures that such information is used or transmitted only in accordance with established privacy requirements.

References

FIPS Publication 199
NIST Special Publication 800-41
NIST Special Publication 800-77

TRANSMISSION CONFIDENTIALITY AND INTEGRITY

name: SC-8

statement

Protect the [Selection (one or more): confidentiality; integrity] of transmitted information.

guidance

This control applies to internal and external networks and any system components that can transmit information including, for example, servers, notebook computers, desktop computers, mobile devices, printers, copiers, scanners, facsimile machines, and radios. Unprotected communication paths are exposed to the possibility of interception and modification. Protecting the confidentiality and integrity of information can be accomplished by physical means or by logical means. Physical protection can be achieved by employing protected distribution systems. Logical protection can be achieved by employing encryption techniques. Organizations relying on commercial providers offering transmission services as commodity services rather than as

fully dedicated services, may find it difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality and integrity. In such situations, organizations determine what types of confidentiality/integrity services are available in standard, commercial telecommunication service packages. If it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, organizations can implement appropriate compensating security controls or explicitly accept the additional risk.

CRYPTOGRAPHIC PROTECTION

name: SC-8 (1)

statement

Implement cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.

guidance

Encrypting information for transmission protects information from unauthorized disclosure and modification. Cryptographic mechanisms implemented to protect information integrity include, for example, cryptographic hash functions which have common application in digital signatures, checksums, and message authentication codes.

PRE- AND POST-TRANSMISSION HANDLING

name: SC-8 (2)

statement

Maintain the [Selection (one or more): confidentiality; integrity] of information during preparation for transmission and during reception.

guidance

Information can be either unintentionally or maliciously disclosed or modified during preparation for transmission or during reception including, for example, during aggregation, at protocol transformation points, and during packing and unpacking. These unauthorized disclosures or modifications compromise the confidentiality or integrity of the information.

CRYPTOGRAPHIC PROTECTION FOR MESSAGE EXTERNALS

organization-defined alternative physical safeguards
organization-defined alternative physical safeguards

name: SC-8 (3)

statement

Implement cryptographic mechanisms to protect message externals unless otherwise protected by .

guidance

This control enhancement addresses protection against unauthorized disclosure of information. Message externals include, for example, message headers and routing information. This control enhancement prevents the exploitation of message externals and applies to internal and external networks or links that may be visible to individuals who are not authorized users. Header and routing information is sometimes transmitted in the clear (i.e., unencrypted) because the information is not properly identified by organizations as having significant value or because encrypting the information can result in lower network performance or higher costs. Alternative physical safeguards include, for example, protected distribution systems.

CONCEAL OR RANDOMIZE COMMUNICATIONS

organization-defined alternative physical safeguards
organization-defined alternative physical safeguards
name: SC-8 (4)

statement

Implement cryptographic mechanisms to conceal or randomize communication patterns unless otherwise protected by .

guidance

This control enhancement addresses protection against unauthorized disclosure of information. Communication patterns include, for example, frequency, periods, amount, and predictability. Changes to communications patterns can reveal information having intelligence value especially when combined with other available information related to the missions and business functions supported by organizational systems. This control enhancement prevents the derivation of intelligence based on communications patterns and applies to internal and external networks or links that may be visible to individuals who are not authorized users. Encrypting the links and transmitting in continuous, fixed or random patterns prevents the derivation of intelligence from the system communications patterns. Alternative physical safeguards include, for example, protected distribution systems.

References

FIPS Publication 140-2
FIPS Publication 197
NIST Special Publication 800-52
NIST Special Publication 800-77
NIST Special Publication 800-81
NIST Special Publication 800-113

TRANSMISSION CONFIDENTIALITY

name: SC-9

statement

Incorporated into SC-8.

NETWORK DISCONNECT

organization-defined time-period
organization-defined time-period
name: SC-10

statement

Terminate the network connection associated with a communications session at the end of the session or after of inactivity.

guidance

This control applies to internal and external networks. Terminating network connections associated with specific communications sessions include, for example, de-allocating associated TCP/IP address or port pairs at the operating system level and de-allocating networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. Periods of inactivity may be established by organizations and include, for example, time-periods by type of network access or for specific network accesses.

TRUSTED PATH

organization-defined security functions
organization-defined security functions
name: SC-11

statement

item
name: SC-11a.

Provide a [Selection: physically; logically] isolated trusted communications path for communications between the user and the trusted components of the system; and

item
name: SC-11b.

Permit users to invoke the trusted communications path for communications between the user and the following security functions of the system, including at a minimum, authentication and re-authentication: .

guidance

Trusted paths are mechanisms by which users (through input devices) can communicate directly with security functions of systems with the requisite assurance to support security policies. These mechanisms can be activated only by users or the security functions of organizational systems. User responses via trusted paths are protected from modifications by or disclosure to untrusted applications. Organizations employ trusted paths for trustworthy, high-assurance connections between security functions of systems and users including, for example, during system logons. The original implementations of trusted path used an out-of-band signal to initiate the path, for example using the <BREAK> key, which does not transmit characters that can be spoofed. In later implementations, a key combination that could not be hijacked was used, for example, the <CTRL> + <ALT> + <DEL> keys. Note, however, that any such key combinations are platform-specific and may not provide a trusted path implementation in every case. Enforcement of trusted communications paths is typically provided by a specific implementation that meets the reference monitor concept.

LOGICAL ISOLATION

organization-defined security functions
organization-defined security functions
name: SC-11 (1)

statement

item
name: SC-11 (1)(a)

Provide a trusted communications path that is irrefutably distinguishable from other communications paths; and

item
name: SC-11 (1)(b)

Initiate the trusted communications path for communications between the following security functions of the system and the user .

guidance

This enhancement permits the system to initiate a trusted path which necessitates that the user can unmistakably recognize the source of the communication as a trusted system component. For example, the trusted path may appear in an area of the display that other applications cannot access, or be based on the presence of an identifier that cannot be spoofed.

None

CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

organization-defined requirements for key generation, distribution, storage, access, and destruction
organization-defined requirements for key generation, distribution, storage, access, and destruction
name: SC-12

statement

Establish and manage cryptographic keys for required cryptography employed within the system in accordance with .

guidance

Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. Organizations define their key management requirements in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines, specifying appropriate options, levels, and parameters. Organizations manage trust stores to ensure that only approved trust anchors are in such trust stores. This includes certificates with visibility external to organizational systems and certificates related to the internal operations of systems.

AVAILABILITY

name: SC-12 (1)

statement

Maintain availability of information in the event of the loss of cryptographic keys by users.

guidance

Escrowing of encryption keys is a common practice for ensuring availability in the event of loss of keys. A forgotten passphrase is an example of losing a cryptographic key.
None

SYMMETRIC KEYS

name: SC-12 (2)

statement

Produce, control, and distribute symmetric cryptographic keys using [Selection: NIST FIPS-compliant; NSA-approved] key management technology and processes.

guidance

None.
None

ASYMMETRIC KEYS

name: SC-12 (3)

statement

Produce, control, and distribute asymmetric cryptographic keys using [Selection: NSA-approved key management technology and processes; approved DoD PKI Class 3 certificates; prepositioned keying material; approved DoD PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user#s private key; certificates issued in accordance with organization-defined requirements].

guidance

None.
None

PKI CERTIFICATES

name: SC-12 (4)

statement

Incorporated into SC-12.

PKI CERTIFICATES / HARDWARE TOKENS

name: SC-12 (5)

statement

Incorporated into SC-12.

CRYPTOGRAPHIC PROTECTION

organization-defined cryptographic uses and type of cryptography required for each use
organization-defined cryptographic uses and type of cryptography required for each use
name: SC-13

statement

Implement the following cryptographic uses and type of cryptography for each use: .

guidance

Cryptography can be employed to support a variety of security solutions including, for example, the protection of classified information and Controlled Unclassified Information; the provision and implementation of digital signatures; and the enforcement of information separation when authorized individuals have the necessary clearances but lack the necessary formal

access approvals. Cryptography can also be used to support random number generation and hash generation. Generally applicable cryptographic standards include FIPS-validated cryptography and NSA-approved cryptography. This control does not impose any requirements on organizations to use cryptography. However, if cryptography is required due to the selection of other security controls, organizations define each type of cryptographic use and the type of cryptography required. For example, organizations that need to protect classified information specify the use of NSA-approved cryptography. Organizations that need to provision and implement digital signatures specify the use of FIPS-validated cryptography. In all instances, cryptography is implemented in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidelines.

FIPS-VALIDATED CRYPTOGRAPHY

name: SC-13 (1)

statement

Incorporated into SC-13.

NSA-APPROVED CRYPTOGRAPHY

name: SC-13 (2)

statement

Incorporated into SC-13.

INDIVIDUALS WITHOUT FORMAL ACCESS APPROVALS

name: SC-13 (3)

statement

Incorporated into SC-13.

DIGITAL SIGNATURES

name: SC-13 (4)

statement

Incorporated into SC-13.

References

FIPS Publication 140-2

PUBLIC ACCESS PROTECTIONS

name: SC-14

statement

Incorporated into AC-2, AC-3, AC-5, AC-6, SI-3, SI-4, SI-5, SI-7, SI-10.

COLLABORATIVE COMPUTING DEVICES AND APPLICATIONS

organization-defined exceptions where remote activation is to be allowed
organization-defined exceptions where remote activation is to be allowed
name: SC-15

statement

item
name: SC-15a.

Prohibit remote activation of collaborative computing devices and applications with the following exceptions: ; and

item
name: SC-15b.

Provide an explicit indication of use to users physically present at the devices.

guidance

Collaborative computing devices and applications include, for example, remote meeting devices and applications, networked white boards, cameras, and microphones. Explicit indication of use includes, for example, signals to users when collaborative computing devices and applications are activated.

PHYSICAL DISCONNECT

name: SC-15 (1)

statement

Provide physical disconnect of collaborative computing devices in a manner that supports ease of use.

guidance

Failing to physically disconnect from collaborative computing devices can result in subsequent compromises of organizational information. Providing easy methods to physically disconnect from such devices after a collaborative computing session ensures that participants carry out the disconnect activity without having to go through complex and tedious procedures.
None

BLOCKING INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC

name: SC-15 (2)

statement

Incorporated into SC-7.

DISABLING AND REMOVAL IN SECURE WORK AREAS

organization-defined systems or system components
organization-defined systems or system components

organization-defined secure work areas
organization-defined secure work areas
name: SC-15 (3)

statement

Disable or remove collaborative computing devices and applications from in .

guidance

Failing to disable or remove collaborative computing devices and applications from systems or system components can result in subsequent compromises of organizational information including, for example, eavesdropping on conversations.
None

EXPLICITLY INDICATE CURRENT PARTICIPANTS

organization-defined online meetings and teleconferences
organization-defined online meetings and teleconferences
name: SC-15 (4)

statement

Provide an explicit indication of current participants in .

guidance

This control enhancement helps to prevent unauthorized individuals from participating in collaborative computing sessions without the explicit knowledge of other participants.
None

TRANSMISSION OF SECURITY AND PRIVACY ATTRIBUTES

organization-defined security and privacy attributes
organization-defined security and privacy attributes
name: SC-16

statement

Associate with information exchanged between systems and between system components.

guidance

Security and privacy attributes can be explicitly or implicitly associated with the information contained in systems or system components. Attributes are an abstraction representing the basic properties or characteristics of an entity with respect to safeguarding information or the management of personally identifiable information. Attributes are typically associated with internal data structures including, for example, records, buffers, files within the information system. Security and privacy attributes are used to implement access control and flow control policies; reflect special dissemination, management, or distribution instructions, including permitted uses of personally identifiable information; or support other aspects of the information security and privacy policies. Privacy attributes may be used independently, or in conjunction with security attributes.

INTEGRITY VALIDATION

name: SC-16 (1)

statement

Validate the integrity of transmitted security and privacy attributes.

guidance

This control enhancement ensures that the integrity verification of transmitted information includes security and privacy attributes.

PUBLIC KEY INFRASTRUCTURE CERTIFICATES

organization-defined certificate policy
organization-defined certificate policy
name: SC-17

statement

Issue public key certificates under an or obtain public key certificates from an approved service provider.

guidance

For all certificates, organizations manage system trust stores to ensure only approved trust anchors are in the trust stores. This control addresses certificates with visibility external to organizational systems and certificates related to the internal operations of systems, for example, application-specific time services.

References

NIST Special Publication 800-32
NIST Special Publication 800-63

MOBILE CODE

name: SC-18

statement

item
name: SC-18a.

Define acceptable and unacceptable mobile code and mobile code technologies;

item
name: SC-18b.

Establish usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and

item
name: SC-18c.

Authorize, monitor, and control the use of mobile code within the system.

guidance

Decisions regarding the use of mobile code within organizational systems are based on the potential for the code to cause damage to the systems if used maliciously. Mobile code technologies include, for example, Java, JavaScript, ActiveX, Postscript, PDF, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidelines apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations and devices including, for example, notebook computers and smart phones. Mobile code policy and procedures address the specific actions taken to prevent the development, acquisition, and introduction of unacceptable mobile code within organizational systems.

IDENTIFY UNACCEPTABLE CODE AND TAKE CORRECTIVE ACTIONS

organization-defined unacceptable mobile code
organization-defined unacceptable mobile code

organization-defined corrective actions
organization-defined corrective actions

name: SC-18 (1)

statement

Identify and take .

guidance

Corrective actions when unacceptable mobile code is detected include, for example, blocking, quarantine, or alerting administrators. Blocking includes, for example, preventing transmission of word processing files with embedded macros when such macros have been defined to be unacceptable mobile code.
None

ACQUISITION, DEVELOPMENT, AND USE

organization-defined mobile code requirements
organization-defined mobile code requirements
name: SC-18 (2)

statement

Verify that the acquisition, development, and use of mobile code to be deployed in the system meets .

guidance

None.
None

PREVENT DOWNLOADING AND EXECUTION

organization-defined unacceptable mobile code
organization-defined unacceptable mobile code
name: SC-18 (3)

statement

Prevent the download and execution of .

guidance

None.
None

PREVENT AUTOMATIC EXECUTION

organization-defined software applications
organization-defined software applications

organization-defined actions
organization-defined actions
name: SC-18 (4)

statement

Prevent the automatic execution of mobile code in and enforce prior to executing the code.

guidance

Actions enforced before executing mobile code, include, for example, prompting users prior to opening electronic mail attachments. Preventing automatic execution of mobile code includes, for example, disabling auto execute features on system components employing portable storage devices such as Compact Disks (CDs), Digital Video Disks (DVDs), and Universal Serial Bus (USB) devices.
None

ALLOW EXECUTION ONLY IN CONFINED ENVIRONMENTS

name: SC-18 (5)

statement

Allow execution of permitted mobile code only in confined virtual machine environments.

guidance

None.

References
NIST Special Publication 800-28

VOICE OVER INTERNET PROTOCOL

name: SC-19

statement

item
name: SC-19a.

Establish usage restrictions and implementation guidelines for Voice over Internet Protocol (VoIP) technologies; and

item
name: SC-19b.

Authorize, monitor, and control the use of VoIP technologies within the system.

guidance

Usage restrictions and implementation guidelines are based on the potential for the VoIP technology to cause damage to the system if used maliciously.

References

NIST Special Publication 800-58

SECURE NAME/ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)

name: SC-20

statement

item
name: SC-20a.

Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and

item
name: SC-20b.

Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

guidance

This control enables external clients including, for example, remote Internet clients, to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service. Systems that provide name and address resolution services include, for example, domain name system (DNS) servers. Additional artifacts include, for example, DNS Security (DNSSEC) digital signatures and cryptographic keys. DNS resource records are examples of authoritative data. The means to indicate the security status of child zones includes, for example, the use of delegation signer resource records in the DNS. Systems that use technologies other than the DNS to map between host and service names and network addresses provide other means to assure the authenticity and integrity of response data.

CHILD SUBSPACES

name: SC-20 (1)

statement

Incorporated into SC-20.

DATA ORIGIN AND INTEGRITY

name: SC-20 (2)

statement

Provide data origin and integrity protection artifacts for internal name/address resolution queries.

guidance

None.
None

References

FIPS Publication 140-2
NIST Special Publication 800-81

SECURE NAME/ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)

name: SC-21

statement

Request and perform data origin authentication and data integrity verification on the name/ address resolution responses the system receives from authoritative sources.

guidance

Each client of name resolution services either performs this validation on its own, or has authenticated channels to trusted validation providers. Systems that provide name and address resolution services for local clients include, for example, recursive resolving or caching domain name system (DNS) servers. DNS client resolvers either perform validation of DNSSEC signatures, or clients use authenticated channels to recursive resolvers that perform such validations. Systems that use technologies other than the DNS to map between host/ service names and network addresses provide some other means to enable clients to verify the authenticity and integrity of response data.

DATA ORIGIN AND INTEGRITY

name: SC-21 (1)

statement

Incorporated into SC-21.

References

NIST Special Publication 800-81

ARCHITECTURE AND PROVISIONING FOR NAME/ADDRESS RESOLUTION SERVICE

name: SC-22

statement

Ensure the systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal and external role separation.

guidance

Systems that provide name and address resolution services include, for example, domain name system (DNS) servers. To eliminate single points of failure and to enhance redundancy, organizations employ at least two authoritative domain name system servers; one configured as the primary server and the other configured as the secondary server. Additionally, organizations typically deploy the servers in two geographically separated network subnetworks (i.e., not located in the same physical facility). For role separation, DNS servers with internal roles only process name and address resolution requests from within organizations (i.e., from internal clients). DNS servers with external roles only process name and address resolution information requests from clients external to organizations (i.e., on external networks including the Internet). Organizations specify clients that can access authoritative DNS servers in certain roles, for example, by address ranges and explicit lists.

References

NIST Special Publication 800-81

SESSION AUTHENTICITY

name: SC-23

statement

Protect the authenticity of communications sessions.

guidance

This control addresses communications protection at the session, versus packet level. Such protection establishes grounds for confidence at both ends of communications sessions in the ongoing identities of other parties and in the validity of information transmitted. Authenticity protection includes, for example, protecting against man-in-the-middle attacks and session hijacking, and the insertion of false information into sessions.

INVALIDATE SESSION IDENTIFIERS AT LOGOUT

name: SC-23 (1)

statement

Invalidate session identifiers upon user logout or other session termination.

guidance

This control enhancement curtails the ability of adversaries from capturing and continuing to employ previously valid session IDs.
None

USER-INITIATED LOGOUTS AND MESSAGE DISPLAYS

name: SC-23 (2)
AC-12(1)

statement

Incorporated into AC-12(1).

UNIQUE SESSION IDENTIFIERS WITH RANDOMIZATION

organization-defined randomness requirements
organization-defined randomness requirements
name: SC-23 (3)

statement

Generate a unique session identifier for each session with and recognize only session identifiers that are system-generated.

guidance

This control enhancement curtails the ability of adversaries from reusing previously valid session IDs. Employing the concept of randomness in the generation of unique session identifiers protects against brute-force attacks to determine future session identifiers.

UNIQUE SESSION IDENTIFIERS WITH RANDOMIZATION

name: SC-23 (4)
SC-23(3)

statement

Incorporated into SC-23(3).

ALLOWED CERTIFICATE AUTHORITIES

organization-defined certificate authorities
organization-defined certificate authorities
name: SC-23 (5)

statement

Only allow the use of for verification of the establishment of protected sessions.

guidance

Reliance on certificate authorities (CAs) for the establishment of secure sessions includes, for example, the use of Transport Layer Security (TLS) certificates. These certificates, after verification by their respective CAs, facilitate the establishment of protected sessions between web clients and web servers.

References

NIST Special Publication 800-52
NIST Special Publication 800-77
NIST Special Publication 800-95
NIST Special Publication 800-113

FAIL IN KNOWN STATE

organization-defined known system state
organization-defined known system state

organization-defined types of system failures
organization-defined types of system failures

organization-defined system state information
organization-defined system state information
name: SC-24

statement

Fail to a for preserving in failure.

guidance

Failure in a known state addresses security concerns in accordance with the mission and business needs of organizations. Failure in a known state helps to prevent the loss of confidentiality, integrity, or availability of information in the event of failures of organizational systems or system components. Failure in a known safe state helps to prevent systems from failing to a state that may cause injury to individuals or destruction to property. Preserving system state information facilitates system restart and return to the operational mode of organizations with less disruption of mission and business processes.

THIN NODES

organization-defined system components
organization-defined system components
name: SC-25

statement

Employ with minimal functionality and information storage.

guidance

The deployment of system components with minimal functionality reduces the need to secure every user endpoint, and may reduce the exposure of information, systems, and services to attacks. Examples of reduced or minimal functionality include, for example, diskless nodes and thin client technologies.

HONEYPOTS

name: SC-26

statement

Include components within organizational systems specifically designed to be the target of malicious attacks for detecting, deflecting, and analyzing such attacks.

guidance

A honeypot is established as a decoy to attract adversaries and to deflect their attacks away from the operational systems supporting organizational missions and business functions. Depending upon the specific usage of the honeypot, consultation with the Office of the General Counsel before deployment may be needed.

DETECTION OF MALICIOUS CODE

name: SC-26 (1)

statement

Incorporated into SC-35.

PLATFORM-INDEPENDENT APPLICATIONS

organization-defined platform-independent applications
organization-defined platform-independent applications

name: SC-27

statement

Include within organizational systems: .

guidance

Platforms are combinations of hardware and software used to run software applications. Platforms include operating systems; the underlying computer architectures; or both. Platform-

independent applications are those applications with the capability to execute on multiple platforms. Such applications promote portability and reconstitution on different platforms. This increases the availability of critical or essential functions within organizations in situations where systems with specific operating systems are under attack.

PROTECTION OF INFORMATION AT REST

organization-defined information
organization-defined information
name: SC-28

statement

Protect the [Selection (one or more): confidentiality; integrity] of at rest.

guidance

This control addresses the confidentiality and integrity of information at rest and covers user information and system information. Information at rest refers to the state of information when it is not in process or in transit and is located on storage devices as specific components of systems. The focus of this control is not on the type of storage device or frequency of access but rather the state of the information. System-related information requiring protection includes, for example, configurations or rule sets for firewalls, gateways, intrusion detection and prevention systems, filtering routers, and authenticator content. Organizations may employ different mechanisms to achieve confidentiality and integrity protections, including the use of cryptographic mechanisms and file share scanning. Integrity protection can be achieved, for example, by implementing Write-Once-Read-Many (WORM) technologies. When adequate protection of information at rest cannot otherwise be achieved, organizations may employ other security controls including, for example, frequent scanning to identify malicious code at rest and secure off-line storage in lieu of online storage.

CRYPTOGRAPHIC PROTECTION

organization-defined information
organization-defined information

organization-defined system components
organization-defined system components
name: SC-28 (1)

statement

Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of when at rest on .

guidance

This control enhancement applies to significant concentrations of digital media in organizational areas designated for media storage. It also applies to limited quantities of media generally associated with system components in operational environments including, for example, portable storage devices, notebook computers, and mobile devices. Selection of cryptographic mechanisms is based on the need to protect the confidentiality and integrity of organizational information. The strength of mechanism is commensurate with the security category or classification of the information. Organizations have the flexibility to encrypt all information on storage devices or encrypt specific data structures including, for example, files, records, or fields. Organizations employing cryptographic mechanisms to protect information at rest also consider cryptographic key management solutions.

OFF-LINE STORAGE

organization-defined information
organization-defined information
name: SC-28 (2)

statement

Remove the following information from online storage and store off-line in a secure location: .

guidance

Removing organizational information from online system storage to off-line storage eliminates the possibility of individuals gaining unauthorized access to the information through a network. Therefore, organizations may choose to move information to off-line storage in lieu of protecting such information in online storage.
None

References
NIST Special Publication 800-111
NIST Special Publication 800-124

HETEROGENEITY

organization-defined system components
organization-defined system components
name: SC-29

statement

Employ a diverse set of information technologies for in the implementation of the system.

guidance

Increasing the diversity of information technologies within organizational systems reduces the impact of potential exploitations or compromises of specific technologies. Such diversity protects against common mode failures, including those failures induced by supply chain attacks. Diversity in information technologies also reduces the likelihood that the means adversaries use to compromise one system component will be equally effective against other system components, thus further increasing the adversary work factor to successfully complete planned attacks. An increase in diversity may add complexity and management overhead which could ultimately lead to mistakes and unauthorized configurations.

VIRTUALIZATION TECHNIQUES

organization-defined frequency
organization-defined frequency
name: SC-29 (1)

statement

Employ virtualization techniques to support the deployment of a diversity of operating systems and applications that are changed .

guidance

While frequent changes to operating systems and applications pose configuration management challenges, the changes can result in an increased work factor for adversaries to conduct successful attacks. Changing virtual operating systems or applications, as opposed to changing actual operating systems or applications, provides virtual changes that impede attacker success while reducing configuration management efforts. Virtualization techniques can assist in isolating untrustworthy software or software of dubious provenance into confined execution environments.
None

CONCEALMENT AND MISDIRECTION

organization-defined concealment and misdirection techniques
organization-defined concealment and misdirection techniques

organization-defined systems
organization-defined systems

organization-defined time-periods
organization-defined time-periods
name: SC-30

statement

Employ for at to confuse and mislead adversaries.

guidance

Concealment and misdirection techniques can significantly reduce the targeting capability of adversaries (i.e., window of opportunity and available attack surface) to initiate and complete attacks. For example, virtualization techniques provide organizations with the ability to disguise systems, potentially reducing the likelihood of successful attacks without the cost of having multiple platforms. Increased use of concealment and misdirection techniques and methods including, for example, randomness, uncertainty, and virtualization, may sufficiently confuse and mislead adversaries and subsequently increase the risk of discovery and/or exposing tradecraft. Concealment and misdirection techniques may also provide organizations additional time to successfully perform core missions and business functions. Because of the time and effort required to support concealment and misdirection techniques, it is anticipated that such techniques would be used by organizations on a very limited basis.

VIRTUALIZATION TECHNIQUES

name: SC-30 (1)
SC-29(1)

statement

Incorporated into SC-29(1).

RANDOMNESS

organization-defined techniques
organization-defined techniques
name: SC-30 (2)

statement

Employ to introduce randomness into organizational operations and assets.

guidance

Randomness introduces increased levels of uncertainty for adversaries regarding the actions organizations take in defending their systems against attacks. Such actions may impede the ability of adversaries to correctly target information resources of organizations supporting critical missions or business functions. Uncertainty may also cause adversaries to hesitate before initiating or continuing their attacks. Misdirection techniques involving randomness include, for example, performing certain routine actions at different times of day, employing different information technologies, using different suppliers, and rotating roles and responsibilities of organizational personnel.
None

CHANGE PROCESSING AND STORAGE LOCATIONS

organization-defined processing and/or storage
organization-defined processing and/or storage

organization-defined time frequency
organization-defined time frequency
name: SC-30 (3)

statement

Change the location of [Selection: ; at random time intervals]].

guidance

Adversaries target critical missions and business functions and the systems supporting those missions and functions while at the same time, trying to minimize exposure of their existence and tradecraft. The static, homogeneous, and deterministic nature of organizational systems targeted by adversaries, make such systems more susceptible to attacks with less adversary cost and effort to be successful. Changing processing and storage locations (sometimes referred to as moving target defense) addresses the advanced persistent threat (APT) using techniques such as virtualization, distributed processing, and replication. This enables organizations to relocate the system components (i.e., processing and/or storage) supporting critical missions and business functions. Changing the locations of processing activities and/or storage sites introduces a degree of uncertainty into the targeting activities by adversaries. This uncertainty increases the work factor of adversaries making compromises or breaches to organizational systems much more difficult and time-consuming. It also increases the chances that adversaries may inadvertently disclose aspects of tradecraft while attempting to locate critical organizational resources.
None

MISLEADING INFORMATION

organization-defined system components
organization-defined system components
name: SC-30 (4)

statement

Employ realistic, but misleading information in about its security state or posture.

guidance

This control enhancement misleads potential adversaries regarding the nature and extent of security safeguards deployed by organizations. Thus, adversaries may employ incorrect and ineffective, attack techniques. One way of misleading adversaries is for organizations to place misleading information regarding the specific controls deployed in external systems that

are known to be targeted by adversaries. Another technique is the use of deception nets that mimic actual aspects of organizational systems but use, for example, out-of-date software configurations.
None

CONCEALMENT OF SYSTEM COMPONENTS

organization-defined techniques
organization-defined techniques

organization-defined system components
organization-defined system components
name: SC-30 (5)

statement

Employ to hide or conceal .

guidance

By hiding, disguising, or concealing critical system components, organizations may be able to decrease the probability that adversaries target and successfully compromise those assets. Potential means for organizations to hide, disguise, or conceal system components include, for example, configuration of routers or the use of honeynets or virtualization techniques.
None

COVERT CHANNEL ANALYSIS
name: SC-31

statement

item
name: SC-31a.

Perform a covert channel analysis to identify those aspects of communications within the system that are potential avenues for covert [Selection (one or more): storage; timing] channels; and

item
name: SC-31b.

Estimate the maximum bandwidth of those channels.

guidance

Developers are in the best position to identify potential areas within systems that might lead to covert channels. Covert channel analysis is a meaningful activity when there is the potential

for unauthorized information flows across handling caveats, discretionary policies, or security domains, for example, in the case of systems containing export-controlled information and having connections to external networks (i.e., networks that are not controlled by organizations). Covert channel analysis is also useful for multilevel secure systems, multiple security level systems, and cross-domain systems.

TEST COVERT CHANNELS FOR EXPLOITABILITY

name: SC-31 (1)

statement

Test a subset of the identified covert channels to determine which channels are exploitable.

guidance

None.
None

MAXIMUM BANDWIDTH

organization-defined values
organization-defined values
name: SC-31 (2)

statement

Reduce the maximum bandwidth for identified covert [Selection (one or more); storage; timing] channels to .

guidance

None.
None

MEASURE BANDWIDTH IN OPERATIONAL ENVIRONMENTS

organization-defined subset of identified covert channels
organization-defined subset of identified covert channels
name: SC-31 (3)

statement

Measure the bandwidth of in the operational environment of the system.

guidance

This control enhancement addresses covert channel bandwidth in operational environments versus developmental environments. Measuring covert channel bandwidth in specified operational environments helps organizations to determine how much information can be

covertly leaked before such leakage adversely affects missions or business functions. Covert channel bandwidth may be significantly different when measured in those settings that are independent of the specific environments of operation including, for example, laboratories or development environments.
None

SYSTEM PARTITIONING

organization-defined system components
organization-defined system components

organization-defined circumstances for physical separation of components
organization-defined circumstances for physical separation of components
name: SC-32

statement

Partition the system into residing in separate physical domains or environments based on .

guidance

System partitioning is a part of a defense-in-depth protection strategy. Organizations determine the degree of physical separation of system components from physically distinct components in separate racks in the same room, to components in separate rooms for the more critical components, to significant geographical separation of the most critical components. Security categorization can guide the selection of appropriate candidates for domain partitioning. Managed interfaces restrict or prohibit network access and information flow among partitioned system components.

References

FIPS Publication 199

TRANSMISSION PREPARATION INTEGRITY

name: SC-33

statement

Incorporated into SC-8.

NON-MODIFIABLE EXECUTABLE PROGRAMS

organization-defined system components
organization-defined system components

organization-defined applications
organization-defined applications
name: SC-34

statement

At :

item
name: SC-34a.

Load and execute the operating environment from hardware-enforced, read-only media; and

item
name: SC-34b.

Load and execute from hardware-enforced, read-only media.

guidance

The operating environment for a system contains the specific code that hosts applications, for example, operating systems, executives, or monitors including virtual machine monitors (i.e., hypervisors). It can also include certain applications running directly on hardware platforms. Hardware-enforced, read-only media include, for example, Compact Disk-Recordable (CD-R) and Digital Video Disk-Recordable (DVD-R) disk drives and one-time programmable read-only memory. The use of non-modifiable storage ensures the integrity of software from the point of creation of the read-only image. The use of reprogrammable read-only memory can be accepted as read-only media provided integrity can be adequately protected from the point of initial writing to the insertion of the memory into the system; and there are reliable hardware protections against reprogramming the memory while installed in organizational systems.

NO WRITABLE STORAGE

organization-defined system components
organization-defined system components
name: SC-34 (1)

statement

Employ with no writeable storage that is persistent across component restart or power on/off.

guidance

This control enhancement eliminates the possibility of malicious code insertion via persistent, writeable storage within the designated system components. It applies to fixed and removable storage, with the latter being addressed either directly or as specific restrictions imposed through access controls for mobile devices.

INTEGRITY PROTECTION ON READ-ONLY MEDIA

name: SC-34 (2)

statement

Protect the integrity of information prior to storage on read-only media and control the media after such information has been recorded onto the media.

guidance

Security safeguards prevent the substitution of media into systems or the reprogramming of programmable read-only media prior to installation into the systems. Such safeguards include, for example, a combination of prevention, detection, and response.

HARDWARE-BASED PROTECTION

organization-defined system firmware components
organization-defined system firmware components

organization-defined authorized individuals
organization-defined authorized individuals

name: SC-34 (3)

statement

item

name: SC-34 (3)(a)

Employ hardware-based, write-protect for ; and

item

name: SC-34 (3)(b)

Implement specific procedures for to manually disable hardware write-protect for firmware modifications and re-enable the write-protect prior to returning to operational mode.

guidance

None.
None

HONEYCLIENTS

name: SC-35

statement

Include system components that proactively seek to identify network-based malicious code, malicious websites, or web-based malicious code.

guidance

Honeyclients differ from honeypots in that the components actively probe networks including, the Internet, in search of malicious code contained on external websites. Like honeypots, honeyclients require some supporting isolation measures to ensure that any malicious code discovered during the search and subsequently executed does not infect organizational systems. Virtualization is a common technique for achieving such isolation.

DISTRIBUTED PROCESSING AND STORAGE

organization-defined processing and storage components
organization-defined processing and storage components
name: SC-36

statement

Distribute across multiple physical locations.

guidance

Distributing processing and storage across multiple physical locations provides some degree of redundancy or overlap for organizations, and therefore increases the work factor of adversaries to adversely impact organizational operations, assets, and individuals. This control does not assume a single primary processing or storage location, and therefore, allows for parallel processing and storage.

POLLING TECHNIQUES

organization-defined distributed processing and storage components
organization-defined distributed processing and storage components

organization-defined action
organization-defined action
name: SC-36 (1)

statement

item
name: SC-36 (1)(a)

Employ polling techniques to identify potential faults, errors, or compromises to ; and

item

name: SC-36 (1)(b)

Take in response to identified faults, errors, or compromises.

guidance

Distributed processing and/or storage may be employed to reduce opportunities for adversaries to successfully compromise the confidentiality, integrity, or availability of information and systems. However, distribution of processing and/or storage components does not prevent adversaries from compromising one (or more) of the distributed components. Polling compares the processing results and/or storage content from the various distributed components and subsequently voting on the outcomes. Polling identifies potential faults, errors, or compromises in distributed processing and storage components. Polling techniques may also be applied to processing and storage components that are not physically distributed.

OUT-OF-BAND CHANNELS

organization-defined out-of-band channels
organization-defined out-of-band channels

organization-defined information, system components, or devices
organization-defined information, system components, or devices

organization-defined individuals or systems
organization-defined individuals or systems

name: SC-37

statement

Employ for the physical delivery or electronic transmission of to .

guidance

Out-of-band channels include, for example, local nonnetwork accesses to systems; network paths physically separate from network paths used for operational traffic; or nonelectronic paths such as the US Postal Service. This is in contrast with using the same channels (i.e., in-band channels) that carry routine operational traffic. Out-of-band channels do not have the same vulnerability or exposure as in-band channels, and therefore, the confidentiality, integrity, or availability compromises of in-band channels will not compromise or adversely affect the out-of-band channels. Organizations may employ out-of-band channels in the delivery or transmission of many organizational items including, for example, identifiers and authenticators; cryptographic key management information; configuration management changes for hardware, firmware, or software; security updates; system and data backups; maintenance information; and malicious code protection updates.

ENSURE DELIVERY AND TRANSMISSION

organization-defined security safeguards
organization-defined security safeguards

organization-defined individuals or systems
organization-defined individuals or systems

organization-defined information, system components, or devices
organization-defined information, system components, or devices
name: SC-37 (1)

statement

Employ to ensure that only receive the .

guidance

Techniques employed by organizations to ensure that only designated systems or individuals receive certain information, system components, or devices include, for example, sending authenticators via an approved courier service but requiring recipients to show some form of government-issued photographic identification as a condition of receipt.
None

OPERATIONS SECURITY

organization-defined operations security safeguards
organization-defined operations security safeguards
name: SC-38

statement

Employ to protect key organizational information throughout the system development life cycle.

guidance

Operations security (OPSEC) is a systematic process by which potential adversaries can be denied information about the capabilities and intentions of organizations by identifying, controlling, and protecting generally unclassified information that specifically relates to the planning and execution of sensitive organizational activities. The OPSEC process involves five steps: identification of critical information; analysis of threats; analysis of vulnerabilities; assessment of risks; and the application of appropriate countermeasures. OPSEC safeguards are applied to organizational systems and the environments in which those systems operate. OPSEC safeguards protect the confidentiality of key information including, for example, limiting the sharing of information with suppliers and potential suppliers of system components and

services, and with other non-organizational elements and individuals. Information critical to organizational mission and business success includes, for example, user identities, element uses, suppliers, supply chain processes, functional and security requirements, system design specifications, testing and evaluation protocols, and security control implementation details.

PROCESS ISOLATION

name: SC-39

statement

Maintain a separate execution domain for each executing process with the system.

guidance

Systems can maintain separate execution domains for each executing process by assigning each process a separate address space. Each system process has a distinct address space so that communication between processes is performed in a manner controlled through the security functions, and one process cannot modify the executing code of another process. Maintaining separate execution domains for executing processes can be achieved, for example, by implementing separate address spaces. This capability is readily available in most commercial operating systems that employ multi-state processor technologies.

HARDWARE SEPARATION

name: SC-39 (1)

statement

Implement hardware separation mechanisms to facilitate process separation.

guidance

Hardware-based separation of system processes is generally less susceptible to compromise than software-based separation, thus providing greater assurance that the separation will be enforced. Hardware separation mechanisms include, for example, hardware memory management.
None

THREAD ISOLATION

organization-defined multi-threaded processing
organization-defined multi-threaded processing
name: SC-39 (2)

statement

Maintain a separate execution domain for each thread in .

guidance

None.
None

WIRELESS LINK PROTECTION

organization-defined wireless links
organization-defined wireless links

organization-defined types of signal parameter attacks or references to sources for such attacks
organization-defined types of signal parameter attacks or references to sources for such attacks
name: SC-40

statement

Protect external and internal from .

guidance

This control applies to internal and external wireless communication links that may be visible to individuals who are not authorized system users. Adversaries can exploit the signal parameters of wireless links if such links are not adequately protected. There are many ways to exploit the signal parameters of wireless links to gain intelligence, deny service, or spoof users of organizational systems. This control reduces the impact of attacks that are unique to wireless systems. If organizations rely on commercial service providers for transmission services as commodity items rather than as fully dedicated services, it may not be possible to implement this control.

ELECTROMAGNETIC INTERFERENCE

organization-defined level of protection
organization-defined level of protection
name: SC-40 (1)

statement

Implement cryptographic mechanisms that achieve against the effects of intentional electromagnetic interference.

guidance

This control enhancement protects against intentional jamming that might deny or impair communications by ensuring that wireless spread spectrum waveforms used to provide anti-jam protection are not predictable by unauthorized individuals. The control enhancement may also coincidentally help to mitigate the effects of unintentional jamming due to interference from legitimate transmitters sharing the same spectrum. Mission requirements, projected threats,

concept of operations, and applicable legislation, directives, regulations, policies, standards, and guidelines determine levels of wireless link availability and performance/cryptography needed.

REDUCE DETECTION POTENTIAL

organization-defined level of reduction
organization-defined level of reduction
name: SC-40 (2)

statement

Implement cryptographic mechanisms to reduce the detection potential of wireless links to .

guidance

This control enhancement is needed for covert communications and protecting wireless transmitters from being geo-located by their transmissions. The control enhancement ensures that spread spectrum waveforms used to achieve low probability of detection are not predictable by unauthorized individuals. Mission requirements, projected threats, concept of operations, and applicable legislation, directives, regulations, policies, standards, and guidelines determine the levels to which wireless links should be undetectable.

IMITATIVE OR MANIPULATIVE COMMUNICATIONS DECEPTION

name: SC-40 (3)

statement

Implement cryptographic mechanisms to identify and reject wireless transmissions that are deliberate attempts to achieve imitative or manipulative communications deception based on signal parameters.

guidance

This control enhancement ensures that the signal parameters of wireless transmissions are not predictable by unauthorized individuals. Such unpredictability reduces the probability of imitative or manipulative communications deception based upon signal parameters alone.

SIGNAL PARAMETER IDENTIFICATION

organization-defined wireless transmitters
organization-defined wireless transmitters
name: SC-40 (4)

statement

Implement cryptographic mechanisms to prevent the identification of by using the transmitter signal parameters.

guidance

Radio fingerprinting techniques identify the unique signal parameters of transmitters to fingerprint such transmitters for purposes of tracking and mission/user identification. This control enhancement protects against the unique identification of wireless transmitters for purposes of intelligence exploitation by ensuring that anti-fingerprinting alterations to signal parameters are not predictable by unauthorized individuals. This control enhancement helps assure mission success when anonymity is required.

PORT AND I/O DEVICE ACCESS

organization-defined connection ports or input/output devices
organization-defined connection ports or input/output devices

organization-defined systems or system components
organization-defined systems or system components
name: SC-41

statement

[Selection: Physically or Logically] disable or remove on .

guidance

Connection ports include, for example, Universal Serial Bus (USB) and Firewire (IEEE 1394). Input/output (I/O) devices include, for example, Compact Disk (CD) and Digital Video Disk (DVD) drives. Disabling or removing such connection ports and I/O devices helps prevent exfiltration of information from systems and the introduction of malicious code into systems from those ports or devices. Physically disabling or removing ports and/or devices is the stronger action.

SENSOR CAPABILITY AND DATA

organization-defined exceptions where remote activation of sensors is allowed
organization-defined exceptions where remote activation of sensors is allowed

organization-defined class of users
organization-defined class of users
name: SC-42

statement

item
name: SC-42a.

Prohibit the remote activation of environmental sensing capabilities on organizational systems or system components with the following exceptions: ; and

item
name: SC-42b.

Provide an explicit indication of sensor use to .

guidance

This control often applies to types of systems or system components characterized as mobile devices, for example, smart phones, tablets, and E-readers. These systems often include sensors that can collect and record data regarding the environment where the system is in use. Sensors that are embedded within mobile devices include, for example, cameras, microphones, Global Positioning System (GPS) mechanisms, and accelerometers. While the sensors on mobiles devices provide an important function, if activated covertly, such devices can potentially provide a means for adversaries to learn valuable information about individuals and organizations. For example, remotely activating the GPS function on a mobile device could provide an adversary with the ability to track the specific movements of an individual.
None

REPORTING TO AUTHORIZED INDIVIDUALS OR ROLES

organization-defined sensors
organization-defined sensors
name: SC-42 (1)

statement

Verify that the system is configured so that data or information collected by the is only reported to authorized individuals or roles.

guidance

In situations where sensors are activated by authorized individuals, it is still possible that the data or information collected by the sensors will be sent to unauthorized entities.
None

AUTHORIZED USE

organization-defined measures
organization-defined measures

organization-defined sensors
organization-defined sensors
name: SC-42 (2)

statement

Employ so that data or information collected by is only used for authorized purposes.

guidance

Information collected by sensors for a specific authorized purpose could be misused for some unauthorized purpose. For example, GPS sensors that are used to support traffic navigation could be misused to track movements of individuals. Measures to mitigate such activities include, for example, additional training to ensure that authorized individuals do not abuse their authority; and in the case where sensor data or information is maintained by external parties, contractual restrictions on the use of such data/information.

PROHIBIT USE OF DEVICES

organization-defined environmental sensing capabilities
organization-defined environmental sensing capabilities

organization-defined facilities, areas, or systems
organization-defined facilities, areas, or systems
name: SC-42 (3)

statement

Prohibit the use of devices possessing in .

guidance

For example, organizations may prohibit individuals from bringing cell phones or digital cameras into certain designated facilities or controlled areas within facilities where classified information is stored or sensitive conversations are taking place.
None

NOTICE OF COLLECTION

organization-defined sensors
organization-defined sensors

organization-defined measures
organization-defined measures
name: SC-42 (4)

statement

Employ the following measures to facilitate an individual#s awareness that personally identifiable information is being collected by : .

guidance

Awareness that organizational sensors are collecting data enable individuals to more effectively engage in managing their privacy. Measures can include, for example, conventional written notices and sensor configurations that make individuals aware directly or indirectly through other devices that the sensor is collecting information. Usability and efficacy of the notice are important considerations.

COLLECTION MINIMIZATION

organization-defined sensors
organization-defined sensors
name: SC-42 (5)

statement

Employ that are configured to minimize the collection of information about individuals that is not needed.

guidance

Although policies to control for authorized use can be applied to information once it is collected, minimizing the collection of information that is not needed mitigates privacy-related risk at the system entry point and mitigates the risk of policy control failures. Sensor configurations include, for example, the obscuring of human features such as blurring or pixelating flesh tones.
None

References

NIST Special Publication 800-124

USAGE RESTRICTIONS

organization-defined system components
organization-defined system components
name: SC-43

statement

item

name: SC-43a.

Establish usage restrictions and implementation guidelines for ; and

item

name: SC-43b.

Authorize, monitor, and control the use of such components within the system.

guidance

This control applies to all system components including wired and wireless peripheral components, for example, copiers, printers, scanners, optical devices, and other similar technologies. Usage restrictions and implementation guidelines are based on the potential for the system components to cause damage to the system if used maliciously. Usage restrictions for other technologies such as VoIP, mobile code, mobile devices, and wireless are addressed in SC-19, SC-18, AC-19, and AC-18.

References

NIST Special Publication 800-124

DETONATION CHAMBERS

organization-defined system, system component, or location
organization-defined system, system component, or location
name: SC-44

statement

Employ a detonation chamber capability within .

guidance

Detonation chambers, also known as dynamic execution environments, allow organizations to open email attachments, execute untrusted or suspicious applications, and execute Universal Resource Locator requests in the safety of an isolated environment or a virtualized sandbox. These protected and isolated execution environments provide a means of determining whether the associated attachments or applications contain malicious code. While related to the concept of deception nets, this control is not intended to maintain a long-term environment in which adversaries can operate and their actions can be observed. Rather, it is intended to quickly identify malicious code and reduce the likelihood that the code is propagated to user environments of operation or prevent such propagation completely.

SYSTEM AND INFORMATION INTEGRITY

SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES

organization-defined personnel or roles
organization-defined personnel or roles

organization-defined senior management official
organization-defined senior management official

organization-defined frequency
organization-defined frequency

organization-defined frequency
organization-defined frequency
name: SI-1

statement

item
name: SI-1a.

Develop, document, and disseminate to :

item
name: SI-1a.1.

A system and information integrity policy that:

item
name: SI-1a.1.(a)

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

item
name: SI-1a.1.(b)

Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and

item
name: SI-1a.2.

Procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls;

item
name: SI-1b.

Designate an to manage the system and information integrity policy and procedures;

item
name: SI-1c.

Review and update the current system and information integrity:

item
name: SI-1c.1.

Policy ; and

item
name: SI-1c.2.

Procedures ;

item
name: SI-1d.

Ensure that the system and information integrity procedures implement the system and information integrity policy and controls; and

item
name: SI-1e.

Develop, document, and implement remediation actions for violations of the system and information integrity policy.

guidance

This control addresses the establishment of policy and procedures for the effective implementation of the controls and control enhancements in the SI family. The risk management strategy is an important factor in establishing policy and procedures. Comprehensive policy and procedures help provide security and privacy assurance. Security and privacy program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general security and privacy policy or can be represented by multiple policies reflecting the complex nature of organizations. The procedures can be established for security and privacy programs and for systems, if needed. Procedures describe how policies or controls are implemented and can be directed at the personnel or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. It is important to recognize that restating controls does not constitute an organizational policy or procedure.

References

NIST Special Publication 800-12
NIST Special Publication 800-100

FLAW REMEDIATION

organization-defined time-period
organization-defined time-period
name: SI-2

statement

item
name: SI-2a.

Identify, report, and correct system flaws;

item
name: SI-2b.

Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;

item
name: SI-2c.

Install security-relevant software and firmware updates within of the release of the updates; and

item
name: SI-2d.

Incorporate flaw remediation into the organizational configuration management process.

guidance

Organizations identify systems affected by software flaws including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security and privacy responsibilities. Security-relevant software updates include, for example, patches, service packs, hot fixes, and anti-virus signatures. Organizations also address flaws discovered during assessments, continuous monitoring, incident response activities, and system error handling. By incorporating flaw remediation into ongoing configuration management processes, required remediation actions can be tracked and verified. Organization-defined time-periods for updating security-relevant software and firmware may vary based on a variety of factors including, for example, the security category of the system or the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw). Some types of flaw remediation may require more testing than other types. Organizations determine the type of testing needed for the specific type of flaw remediation activity under consideration and the types of changes that are to be configuration-managed. In some situations, organizations may determine that testing of software or firmware updates is not necessary or practical, for example, when implementing simple anti-virus signature updates. Organizations also consider in testing decisions, whether security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures.

CENTRAL MANAGEMENT

name: SI-2 (1)

statement

Centrally manage the flaw remediation process.

guidance

Central management is the organization-wide management and implementation of flaw remediation processes. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed flaw remediation controls.

AUTOMATED FLAW REMEDIATION STATUS

organization-defined frequency
organization-defined frequency
name: SI-2 (2)

statement

Employ automated mechanisms to determine the state of system components with regard to flaw remediation.

guidance

None.

TIME TO REMEDIATE FLAWS AND BENCHMARKS FOR CORRECTIVE ACTIONS

organization-defined benchmarks
organization-defined benchmarks
name: SI-2 (3)

statement

item
name: SI-2 (3)(a)

Measure the time between flaw identification and flaw remediation; and

item
name: SI-2 (3)(b)

Establish for taking corrective actions.

guidance

This control enhancement requires organizations to determine the time it takes on the average to correct system flaws after such flaws have been identified, and subsequently establish organizational benchmarks (i.e., time frames) for taking corrective actions. Benchmarks can be established by the type of flaw or the severity of the potential vulnerability if the flaw can be exploited.

None

AUTOMATED PATCH MANAGEMENT TOOLS

name: SI-2 (4)

statement

Incorporated into SI-2.

AUTOMATIC SOFTWARE AND FIRMWARE UPDATES

organization-defined security-relevant software and firmware updates
organization-defined security-relevant software and firmware updates

organization-defined system components
organization-defined system components

name: SI-2 (5)

statement

Install automatically to .

guidance

Due to system integrity and availability concerns, organizations consider the methodology used to carry out automatic updates. Organizations balance the need to ensure that the updates are installed as soon as possible with the need to maintain configuration management and control with any mission or operational impacts that automatic updates might impose.

None

REMOVAL OF PREVIOUS VERSIONS OF SOFTWARE AND FIRMWARE

organization-defined software and firmware components
organization-defined software and firmware components

name: SI-2 (6)

statement

Remove previous versions of after updated versions have been installed.

guidance

Previous versions of software or firmware components that are not removed from the system after updates have been installed may be exploited by adversaries. Some products may remove previous versions of software and firmware automatically from the system.

None

PERSONALLY IDENTIFIABLE INFORMATION

organization-defined time-period
organization-defined time-period
name: SI-2 (7)

statement

item
name: SI-2 (7)(a)

Identify and correct flaws related to the collection, usage, processing, or dissemination of personally identifiable information;

item
name: SI-2 (7)(b)

Report flaws related to personally identifiable information to the Senior Agency Official for Privacy;

item
name: SI-2 (7)(c)

Receive approval for correction of privacy-related flaws from the Senior Agency Official for Privacy;

item
name: SI-2 (7)(d)

Prior to installation, assess software and firmware updates related to flaw remediation for effectiveness and consistency with terms agreed upon in the privacy impact assessment;

item
name: SI-2 (7)(e)

Install privacy-relevant software and firmware updates within of the release of the updates; and

item
name: SI-2 (7)(f)

Incorporate flaw remediation of personally identifiable information into the organizational configuration management process.

guidance

None.

References

FIPS Publication 140-2
NIST Special Publication 800-40
NIST Special Publication 800-128

MALICIOUS CODE PROTECTION

organization-defined frequency
organization-defined frequency

organization-defined action
organization-defined action
name: SI-3

statement

item
name: SI-3a.

Implement [Selection (one or more): signature based; non-signature based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;

item
name: SI-3b.

Automatically update malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures;

item
name: SI-3c.

Configure malicious code protection mechanisms to:

item
name: SI-3c.1.

Perform periodic scans of the system and real-time scans of files from external sources at [Selection (one or more); endpoint; network entry/exit points] as the files are downloaded, opened, or executed in accordance with organizational policy; and

item
name: SI-3c.2.

[Selection (one or more): block malicious code; quarantine malicious code; send alert to administrator;] in response to malicious code detection; and

item
name: SI-3d.

Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.

guidance

System entry and exit points include, for example, firewalls, remote-access servers, workstations, electronic mail servers, web servers, proxy servers, notebook computers, and mobile devices. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats contained within compressed or hidden files, or hidden in files using techniques such as steganography. Malicious code can be inserted into systems in a variety of ways including, for example, by electronic mail, the world-wide web, and portable storage devices. Malicious code insertions occur through the exploitation of system vulnerabilities. A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Malicious code protection mechanisms include, for example, signature- and nonsignature-based technologies. Nonsignature-based detection mechanisms include, for example, artificial intelligence techniques that use heuristics to detect, analyze, and describe the characteristics or behavior of malicious code and to provide safeguards against such code for which signatures do not yet exist or for which existing signatures may not be effective. This includes polymorphic malicious code (i.e., code that changes signatures when it replicates). Nonsignature-based mechanisms also include reputation-based technologies. In addition to the above technologies, pervasive configuration management, comprehensive software integrity controls, and anti-exploitation software may be effective in preventing execution of unauthorized code. Malicious code may be present in commercial off-the-shelf software and in custom-built software. This could include, for example, logic bombs, back doors, and other types of attacks that could affect organizational missions and business functions. In situations where malicious code cannot be detected by detection methods and technologies, organizations rely instead on other types of safeguards including, for example, secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended. Organizations may determine that in response to the detection of malicious code, different actions may be warranted. For example, organizations can define actions in response to malicious code detection during periodic scans, actions in response to detection of malicious downloads, or actions in response to detection of maliciousness when attempting to open or execute files. Due to system integrity and availability concerns, organizations consider the specific methodology used to carry out automatic updates.

CENTRAL MANAGEMENT

name: SI-3 (1)

statement

Centrally manage malicious code protection mechanisms.

guidance

Central management is the organization-wide management and implementation of malicious code protection mechanisms. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed flaw and malicious code protection controls.

AUTOMATIC UPDATES

name: SI-3 (2)

statement

Incorporated into SI-3.

NON-PRIVILEGED USERS

name: SI-3 (3)
AC-6(10)

statement

Incorporated into AC-6(10).

UPDATES ONLY BY PRIVILEGED USERS

name: SI-3 (4)

statement

Update malicious code protection mechanisms only when directed by a privileged user.

guidance

This control enhancement is employed in situations where for reasons of security or operational continuity, updates to malicious code protection mechanisms are only applied when approved by designated organizational personnel.

PORTABLE STORAGE DEVICES

name: SI-3 (5)

statement

Incorporated into MP-7.

TESTING AND VERIFICATION

organization-defined frequency
organization-defined frequency
name: SI-3 (6)

statement

item
name: SI-3 (6)(a)

Test malicious code protection mechanisms by introducing a known benign, non-spreading test case into the system; and

item
name: SI-3 (6)(b)

Verify that the detection of the test case and the associated incident reporting occur.

guidance

None.

NONSIGNATURE-BASED DETECTION

name: SI-3 (7)

statement

Incorporated into SI-3.

DETECT UNAUTHORIZED COMMANDS

organization-defined unauthorized operating system commands
organization-defined unauthorized operating system commands

organization-defined system hardware components
organization-defined system hardware components
name: SI-3 (8)

statement

Detect through the kernel application programming interface at and [Selection (one or more): issue a warning; audit the command execution; prevent the execution of the command].

guidance

This control enhancement can also be applied to critical interfaces other than kernel-based interfaces, including for example, interfaces with virtual machines and privileged applications. Unauthorized operating system commands include, for example, commands for kernel functions from system processes that are not trusted to initiate such commands, or commands for kernel functions that are suspicious even though commands of that type are reasonable for processes to initiate. Organizations can define the malicious commands to be detected by a combination of command types, command classes, or specific instances of commands. Organizations can define hardware components by component type, component, component location in the network, or combination therein. Organizations may select different actions for different types, classes, or instances of malicious commands.

AUTHENTICATE REMOTE COMMANDS

organization-defined security safeguards

organization-defined security safeguards

organization-defined remote commands
organization-defined remote commands
name: SI-3 (9)

statement

Implement to authenticate .

guidance

This control enhancement protects against unauthorized commands and replay of authorized commands. This capability is important for those remote systems whose loss, malfunction, misdirection, or exploitation would have immediate and/or serious consequences, including, for example, injury or death, property damage, loss of high-value assets, compromise of classified or controlled unclassified information, or failure of missions or business functions. Authentication safeguards 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 employed, for example, to authenticate remote commands.

MALICIOUS CODE ANALYSIS

organization-defined tools and techniques
organization-defined tools and techniques
name: SI-3 (10)

statement

item
name: SI-3 (10)(a)

Employ to analyze the characteristics and behavior of malicious code; and

item
name: SI-3 (10)(b)

Incorporate the results from malicious code analysis into organizational incident response and flaw remediation processes.

guidance

The use of malicious code analysis tools provides organizations with a more in-depth understanding of adversary tradecraft (i.e., tactics, techniques, and procedures) and the functionality and purpose of specific instances of malicious code. Understanding the characteristics of malicious code facilitates more effective organizational responses to current

and future threats. Organizations can also conduct malicious code analyses by using reverse engineering techniques or by monitoring the behavior of executing code.
None

SYSTEM MONITORING

organization-defined monitoring objectives
organization-defined monitoring objectives

organization-defined techniques and methods
organization-defined techniques and methods

organization-defined system monitoring information
organization-defined system monitoring information

organization-defined personnel or roles
organization-defined personnel or roles

organization-defined frequency
organization-defined frequency
name: SI-4

statement

item
name: SI-4a.

Monitor the system to detect:

item
name: SI-4a.1.

Attacks and indicators of potential attacks in accordance with ; and

item
name: SI-4a.2.

Unauthorized local, network, and remote connections;

item
name: SI-4b.

Identify unauthorized use of the system through ;

item
name: SI-4c.

Invoke internal monitoring capabilities or deploy monitoring devices:

item
name: SI-4c.1.

Strategically within the system to collect organization-determined essential information; and

item
name: SI-4c.2.

At ad hoc locations within the system to track specific types of transactions of interest to the organization;

item
name: SI-4d.

Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;

item
name: SI-4e.

Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation;

item
name: SI-4f.

Obtain legal opinion regarding system monitoring activities; and

item
name: SI-4g.

Provide to [Selection (one or more): as needed;].

guidance

System monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at system boundaries. Internal monitoring includes the observation of events occurring within the system. Organizations monitor systems, for example, by observing audit activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions. The monitoring objectives guide and inform the determination of the events. System monitoring capability is achieved through a variety of tools and techniques, including, for example, intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, and network monitoring software. The distribution and configuration of monitoring devices can impact throughput at key internal and external boundaries, and at other locations across a network due to the introduction of network throughput latency. Therefore, such devices

are strategically located and deployed as part of an established organization-wide security architecture. Strategic locations for monitoring devices include, for example, selected perimeter locations and near key servers and server farms supporting critical applications. Monitoring devices are typically employed at the managed interfaces associated with controls SC-7 and AC-17. The information collected is a function of the organizational monitoring objectives and the capability of systems to support such objectives. Specific types of transactions of interest include, for example, Hyper Text Transfer Protocol (HTTP) traffic that bypasses HTTP proxies. System monitoring is an integral part of organizational continuous monitoring and incident response programs and output from system monitoring serves as input to those programs. Adjustments to levels of system monitoring are based on law enforcement information, intelligence information, or other credible sources of information. The legality of system monitoring activities is based on applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines.

SYSTEM-WIDE INTRUSION DETECTION SYSTEM

name: SI-4 (1)

statement

Connect and configure individual intrusion detection tools into a system-wide intrusion detection system.

guidance

CM-6.
None

AUTOMATED TOOLS AND MECHANISMS FOR REAL-TIME ANALYSIS

name: SI-4 (2)

statement

Employ automated tools and mechanisms to support near real-time analysis of events.

guidance

Automated tools and mechanisms include, for example, host-based, network-based, transport-based, or storage-based event monitoring tools and mechanisms or Security Information and Event Management technologies that provide real time analysis of alerts and notifications generated by organizational systems.
None

AUTOMATED TOOL AND MECHANISM INTEGRATION

name: SI-4 (3)

statement

Employ automated tools and mechanisms to integrate intrusion detection tools and mechanisms into access control and flow control mechanisms.

guidance

Using automated tools and mechanisms to integrate intrusion detection tools and mechanisms into access and flow control mechanisms facilitates a rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination.
None

INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC

organization-defined frequency
organization-defined frequency
name: SI-4 (4)

statement

Monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.

guidance

Unusual or unauthorized activities or conditions related to system inbound and outbound communications traffic include, for example, internal traffic that indicates the presence of malicious code within organizational systems or propagating among system components; the unauthorized exporting of information; or signaling to external systems. Evidence of malicious code is used to identify potentially compromised systems or system components.
None

SYSTEM-GENERATED ALERTS

organization-defined personnel or roles
organization-defined personnel or roles

organization-defined compromise indicators
organization-defined compromise indicators
name: SI-4 (5)

statement

Alert when the following system-generated indications of compromise or potential compromise occur: .

guidance

Alerts may be generated from a variety of sources, including, for example, audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention

mechanisms, or boundary protection devices such as firewalls, gateways, and routers. Alerts can be automated or they may be transmitted, for example, telephonically, by electronic mail messages, or by text messaging. Organizational personnel on the alert notification list can include, for example, system administrators, mission or business owners, system owners, system security officers, or privacy officers. This control enhancement focuses on the security alerts generated by the system. Alternatively, alerts generated by organizations in SI-4(12) focus on information sources external to the system such as suspicious activity reports and reports on potential insider threats.

RESTRICT NON-PRIVILEGED USERS

name: SI-4 (6)
AC-6(10)

statement

Incorporated into AC-6(10).

AUTOMATED RESPONSE TO SUSPICIOUS EVENTS

organization-defined incident response personnel (identified by name and/or by role)
organization-defined incident response personnel (identified by name and/or by role)

organization-defined least-disruptive actions to terminate suspicious events
organization-defined least-disruptive actions to terminate suspicious events
name: SI-4 (7)

statement

Notify of detected suspicious events and take .

guidance

Least-disruptive actions include, for example, initiating requests for human responses.
None

PROTECTION OF MONITORING INFORMATION

name: SI-4 (8)

statement

Incorporated into SI-4.

TESTING OF MONITORING TOOLS AND MECHANISMS

organization-defined frequency
organization-defined frequency
name: SI-4 (9)

statement

Test intrusion-monitoring tools and mechanisms .

guidance

Testing intrusion-monitoring tools and mechanism is necessary to ensure that the tools and mechanisms are operating correctly and continue to satisfy the monitoring objectives of organizations. The frequency of testing depends on the types of tools and mechanisms used by organizations and the methods of deployment.

VISIBILITY OF ENCRYPTED COMMUNICATIONS

organization-defined encrypted communications traffic
organization-defined encrypted communications traffic

organization-defined system monitoring tools and mechanisms
organization-defined system monitoring tools and mechanisms
name: SI-4 (10)

statement

Make provisions so that is visible to .

guidance

Organizations balance the potentially conflicting needs for encrypting communications traffic and having visibility into such traffic from a monitoring perspective. For some organizations, the need to ensure the confidentiality of communications traffic is paramount; for other organizations, mission assurance is of greater concern. Organizations determine whether the visibility requirement applies to internal encrypted traffic, encrypted traffic intended for external destinations, or a subset of the traffic types.
None

ANALYZE COMMUNICATIONS TRAFFIC ANOMALIES

organization-defined interior points within the system
organization-defined interior points within the system
name: SI-4 (11)

statement

Analyze outbound communications traffic at the external boundary of the system and selected to discover anomalies.

guidance

Examples of organization-defined interior points within the system include subnetworks and subsystems. Anomalies within organizational systems include, for example, large file

transfers; long-time persistent connections; unusual protocols and ports in use; and attempted communications with suspected malicious external addresses.
None

AUTOMATED ORGANIZATION-GENERATED ALERTS

organization-defined personnel or roles
organization-defined personnel or roles

organization-defined activities that trigger alerts
organization-defined activities that trigger alerts
name: SI-4 (12)

statement

Employ automated mechanisms to alert when the following organization-generated indications of inappropriate or unusual activities with security or privacy implications occur: .

guidance

Organizational personnel on the alert notification list can include, for example, system administrators, mission or business owners, system owners, system security officers, or privacy officers. This control enhancement focuses on the security alerts generated by organizations and transmitted using automated means. In contrast to the alerts generated by systems in SI-4(5) that focus on information sources that are internal to the systems such as audit records, the sources of information for this enhancement focus on other entities such as suspicious activity reports and reports on potential insider threats.
None

ANALYZE TRAFFIC AND EVENT PATTERNS

name: SI-4 (13)

statement

item
name: SI-4 (13)(a)

Analyze communications traffic and event patterns for the system;

item
name: SI-4 (13)(b)

Develop profiles representing common traffic and event patterns; and

item
name: SI-4 (13)(c)

Use the traffic and event profiles in tuning system-monitoring devices to reduce the number of false positives and false negatives.

guidance

None.
None

WIRELESS INTRUSION DETECTION

name: SI-4 (14)

statement

Employ a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises or breaches to the system.

guidance

Wireless signals may radiate beyond organization-controlled facilities. Organizations proactively search for unauthorized wireless connections including the conduct of thorough scans for unauthorized wireless access points. Scans are not limited to those areas within facilities containing systems, but also include areas outside of facilities to verify that unauthorized wireless access points are not connected to organizational systems.

WIRELESS TO WIRELINE COMMUNICATIONS

name: SI-4 (15)

statement

Employ an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wireline networks.

guidance

None.

CORRELATE MONITORING INFORMATION

name: SI-4 (16)

statement

Correlate information from monitoring tools and mechanisms employed throughout the system.

guidance

Correlating information from different system monitoring tools and mechanisms can provide a more comprehensive view of system activity. Correlating system monitoring tools and mechanisms that typically work in isolation including, for example, anti-virus software, host monitoring, and network monitoring, can provide an organization-wide monitoring view and may reveal otherwise unseen attack patterns. Understanding capabilities and limitations of

diverse monitoring tools and mechanisms and how to maximize the utility of information generated by those tools and mechanisms can help organizations to develop, operate, and maintain effective monitoring programs.

INTEGRATED SITUATIONAL AWARENESS

name: SI-4 (17)

statement

Correlate information from monitoring physical, cyber, and supply chain activities to achieve integrated, organization-wide situational awareness.

guidance

This control enhancement correlates monitoring information from a more diverse set of information sources to achieve integrated situational awareness. Integrated situational awareness from a combination of physical, cyber, and supply chain monitoring activities enhances the capability of organizations to more quickly detect sophisticated attacks and investigate the methods and techniques employed to carry out such attacks. In contrast to SI-4(16) which correlates the various cyber monitoring information, this control enhancement correlates monitoring beyond the cyber domain. Such monitoring may help reveal attacks on organizations that are operating across multiple attack vectors.

ANALYZE TRAFFIC AND COVERT EXFILTRATION

organization-defined interior points within the system
organization-defined interior points within the system

name: SI-4 (18)

statement

Analyze outbound communications traffic at the external boundary or perimeter of the system and at to detect covert exfiltration of information.

guidance

Examples of organization-defined interior points within the system include subnetworks and subsystems. Covert means that can be used for the exfiltration of information include, for example, steganography.

None

INDIVIDUALS POSING GREATER RISK

organization-defined additional monitoring
organization-defined additional monitoring

organization-defined sources
organization-defined sources

name: SI-4 (19)

statement

Implement of individuals who have been identified by as posing an increased level of risk.

guidance

Indications of increased risk from individuals can be obtained from a variety of sources including, for example, human resource records, intelligence agencies, law enforcement organizations, and other credible sources. The monitoring of specific individuals is closely coordinated with management, legal, security, privacy and human resource officials within organizations conducting such monitoring. Monitoring is conducted in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines.
None

PRIVILEGED USERS

organization-defined additional monitoring
organization-defined additional monitoring
name: SI-4 (20)

statement

Implement of privileged users.

guidance

None.

PROBATIONARY PERIODS

organization-defined additional monitoring
organization-defined additional monitoring

organization-defined probationary period
organization-defined probationary period
name: SI-4 (21)

statement

Implement of individuals during .

guidance

None.

UNAUTHORIZED NETWORK SERVICES

organization-defined authorization or approval processes

organization-defined authorization or approval processes

organization-defined personnel or roles
organization-defined personnel or roles
name: SI-4 (22)

statement

Detect network services that have not been authorized or approved by and [Selection (one or more): audit; alert].

guidance

Unauthorized or unapproved network services include, for example, services in service-oriented architectures that lack organizational verification or validation and therefore may be unreliable or serve as malicious rogues for valid services.

HOST-BASED DEVICES

organization-defined host-based monitoring mechanisms
organization-defined host-based monitoring mechanisms

organization-defined system components
organization-defined system components
name: SI-4 (23)

statement

Implement at .

guidance

System components where host-based monitoring can be implemented include, for example, servers, notebook computers, and mobile devices. Organizations may consider employing host-based monitoring mechanisms from multiple product developers or vendors.

INDICATORS OF COMPROMISE

organization-defined personnel or roles
organization-defined personnel or roles
name: SI-4 (24)

statement

Discover, collect, and distribute to , indicators of compromise.

guidance

Indicators of compromise (IOC) are forensic artifacts from intrusions that are identified on organizational systems at the host or network level. IOCs provide valuable information on systems that have been compromised. IOCs for the discovery of compromised hosts can include, for example, the creation of registry key values. IOCs for network traffic include, for example, Universal Resource Locator or protocol elements that indicate malicious code command and control servers. The rapid distribution and adoption of IOCs can improve information security by reducing the time that systems and organizations are vulnerable to the same exploit or attack.

PERSONALLY IDENTIFIABLE INFORMATION MONITORING

name: SI-4 (25)

statement

Employ automated mechanisms to monitor:

item

name: SI-4 (25)(a)

For unauthorized access or usage of personally identifiable information; and

item

name: SI-4 (25)(b)

The collection, creation, accuracy, relevance, timeliness, impact, and completeness of personally identifiable information.

guidance

Monitoring the collection, creation, accuracy, relevance, timeliness, impact, and completeness of personally identifiable information helps improve data quality. Automated monitoring techniques can create unintended privacy risks because automated controls may connect to external or otherwise unrelated systems. The matching of records between these systems may create linkages with unintended consequences. Organizations assess and document these risks in their privacy impact assessment and make determinations that are in alignment with their privacy program plan.

References

NIST Special Publication 800-61
NIST Special Publication 800-83
NIST Special Publication 800-92
NIST Special Publication 800-94
NIST Special Publication 800-137

SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

organization-defined external organizations

organization-defined external organizations

organization-defined personnel or roles
organization-defined personnel or roles

organization-defined elements within the organization
organization-defined elements within the organization

organization-defined external organizations
organization-defined external organizations
name: SI-5

statement

item
name: SI-5a.

Receive system security alerts, advisories, and directives from on an ongoing basis;

item
name: SI-5b.

Generate internal security alerts, advisories, and directives as deemed necessary;

item
name: SI-5c.

Disseminate security alerts, advisories, and directives to: [Selection (one or more): ; ;]; and

item
name: SI-5d.

Implement security directives in accordance with established time frames, or notify the issuing organization of the degree of noncompliance.

guidance

The United States Computer Emergency Readiness Team (US-CERT) generates security alerts and advisories to maintain situational awareness across the federal government. Security directives are issued by OMB or other designated organizations with the responsibility and authority to issue such directives. Compliance to security directives is essential due to the critical nature of many of these directives and the potential immediate adverse effects on organizational operations and assets, individuals, other organizations, and the Nation should the directives not be implemented in a timely manner. External organizations include, for example, external mission or business partners, supply chain partners, external service providers, and other peer or supporting organizations.

AUTOMATED ALERTS AND ADVISORIES

name: SI-5 (1)

statement

Employ automated mechanisms to make security alert and advisory information available throughout the organization.

guidance

The significant number of changes to organizational systems and the environments in which those systems operate requires the dissemination of security-related information to a variety of organizational entities that have a direct interest in the success of organizational missions and business functions. Based on information provided by security alerts and advisories, changes may be required at one or more of the three tiers related to the management of information security and privacy risk including the governance level, mission and business process level, and the system level.
None

References
NIST Special Publication 800-40

SECURITY AND PRIVACY FUNCTION VERIFICATION

organization-defined security and privacy functions
organization-defined security and privacy functions

organization-defined system transitional states
organization-defined system transitional states

organization-defined frequency
organization-defined frequency

organization-defined personnel or roles
organization-defined personnel or roles

organization-defined alternative action(s)
organization-defined alternative action(s)
name: SI-6

statement

item
name: SI-6a.

Verify the correct operation of ;

item
name: SI-6b.

Perform this verification [Selection (one or more): ; upon command by user with appropriate privilege;];

item
name: SI-6c.

Notify of failed security and privacy verification tests; and

item
name: SI-6d.

[Selection (one or more): Shut the system down; Restart the system;] when anomalies are discovered.

guidance

Transitional states for systems include, for example, system startup, restart, shutdown, and abort. Notifications by the system include, for example, hardware indicator lights, electronic alerts to system administrators, and messages to local computer consoles. In contrast to security function verification, privacy function verification ensures that privacy functions operate as expected and are approved by the Senior Agency Official for Privacy, or that privacy attributes are applied or used as expected.

NOTIFICATION OF FAILED SECURITY TESTS

name: SI-6 (1)

statement

Incorporated into SI-6.

AUTOMATION SUPPORT FOR DISTRIBUTED TESTING

name: SI-6 (2)

statement

Implement automated mechanisms to support the management of distributed security and privacy function testing.

guidance

None.

REPORT VERIFICATION RESULTS

organization-defined personnel or roles

organization-defined personnel or roles
name: SI-6 (3)

statement

Report the results of security and privacy function verification to .

guidance

Organizational personnel with potential interest in the results of the verification of security and privacy function include, for example, system security managers, systems security officers, Senior Agency Information Security Officers, and Senior Agency Officials for Privacy.

SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY

organization-defined software, firmware, and information
organization-defined software, firmware, and information
name: SI-7

statement

Employ integrity verification tools to detect unauthorized changes to .

guidance

Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity. Software includes, for example, operating systems (with key internal components such as kernels, drivers), middleware, and applications. Firmware includes, for example, the Basic Input Output System (BIOS). Information includes personally identifiable information and metadata containing security and privacy attributes associated with information. Integrity-checking mechanisms including, for example, parity checks, cyclical redundancy checks, cryptographic hashes, and associated tools can automatically monitor the integrity of systems and hosted applications.

INTEGRITY CHECKS

organization-defined software, firmware, and information
organization-defined software, firmware, and information

organization-defined transitional states or security-relevant events
organization-defined transitional states or security-relevant events

organization-defined frequency
organization-defined frequency
name: SI-7 (1)

statement

Perform an integrity check of [Selection (one or more): at startup; at ;].

guidance

Security-relevant events include, for example, the identification of a new threat to which organizational systems are susceptible, and the installation of new hardware, software, or firmware. Transitional states include, for example, system startup, restart, shutdown, and abort.
None

AUTOMATED NOTIFICATIONS OF INTEGRITY VIOLATIONS

organization-defined personnel or roles
organization-defined personnel or roles
name: SI-7 (2)

statement

Employ automated tools that provide notification to upon discovering discrepancies during integrity verification.

guidance

The use of automated tools to report integrity violations and to notify organizational personnel in a timely matter is an essential precursor to effective risk response. Personnel having an interest in integrity violations include, for example, mission and business owners, system owners, systems administrators, software developers, systems integrators, and information security officers, and privacy officers.
None

CENTRALLY-MANAGED INTEGRITY TOOLS

name: SI-7 (3)

statement

Employ centrally managed integrity verification tools.

guidance

None.

TAMPER-EVIDENT PACKAGING

name: SI-7 (4)

statement

Incorporated into SA-12.

AUTOMATED RESPONSE TO INTEGRITY VIOLATIONS

organization-defined security safeguards
organization-defined security safeguards
name: SI-7 (5)

statement

Automatically [Selection (one or more): shut the system down; restart the system; implement] when integrity violations are discovered.

guidance

Organizations may define different integrity checking responses by type of information, by specific information, or a combination of both. Examples of types of information include firmware, software, and user data. Examples of specific information include boot firmware for certain types of machines. The automatic implementation of safeguards within organizational systems includes, for example, reversing the changes, halting the system, or triggering audit alerts when unauthorized modifications to critical security files occur.
None

CRYPTOGRAPHIC PROTECTION

name: SI-7 (6)

statement

Implement cryptographic mechanisms to detect unauthorized changes to software, firmware, and information.

guidance

Cryptographic mechanisms used for the protection of integrity include, for example, digital signatures and the computation and application of signed hashes using asymmetric cryptography; protecting the confidentiality of the key used to generate the hash; and using the public key to verify the hash information.

INTEGRATION OF DETECTION AND RESPONSE

organization-defined security-relevant changes to the system
organization-defined security-relevant changes to the system
name: SI-7 (7)

statement

Incorporate the detection of the following unauthorized changes into the organizational incident response capability: .

guidance

This control enhancement helps to ensure that detected events are tracked, monitored, corrected, and available for historical purposes. Maintaining historical records is important both for being able to identify and discern adversary actions over an extended time-period and for possible legal actions. Security-relevant changes include, for example, unauthorized changes to established configuration settings or unauthorized elevation of system privileges.

AUDITING CAPABILITY FOR SIGNIFICANT EVENTS

organization-defined personnel or roles
organization-defined personnel or roles

organization-defined other actions
organization-defined other actions
name: SI-7 (8)

statement

Upon detection of a potential integrity violation, provide the capability to audit the event and initiate the following actions: [Selection (one or more): generate an audit record; alert current user; alert ;].

guidance

Organizations select response actions based on types of software, specific software, or information for which there are potential integrity violations.

VERIFY BOOT PROCESS

organization-defined system components
organization-defined system components
name: SI-7 (9)

statement

Verify the integrity of the boot process of .

guidance

Ensuring the integrity of boot processes is critical to starting system components in known, trustworthy states. Integrity verification mechanisms provide a level of assurance that only trusted code is executed during boot processes.

PROTECTION OF BOOT FIRMWARE

organization-defined security safeguards
organization-defined security safeguards

organization-defined system components

organization-defined system components
name: SI-7 (10)

statement

Implement to protect the integrity of boot firmware in .

guidance

Unauthorized modifications to boot firmware may be indicative of a sophisticated, targeted attack. These types of targeted attacks can result in a permanent denial of service or a persistent malicious code presence. These situations can occur, for example, if the firmware is corrupted or if the malicious code is embedded within the firmware. System components can protect the integrity of boot firmware in organizational systems by verifying the integrity and authenticity of all updates to the firmware prior to applying changes to the system component; and preventing unauthorized processes from modifying the boot firmware.

CONFINED ENVIRONMENTS WITH LIMITED PRIVILEGES

organization-defined user-installed software
organization-defined user-installed software
name: SI-7 (11)

statement

Require that execute in a confined physical or virtual machine environment with limited privileges.

guidance

Organizations identify software that may be of concern regarding its origin or potential for containing malicious code. For this type of software, user installations occur in confined environments of operation to limit or contain damage from malicious code that may be executed.

INTEGRITY VERIFICATION

organization-defined user-installed software
organization-defined user-installed software
name: SI-7 (12)

statement

Require that the integrity of be verified prior to execution.

guidance

Organizations verify the integrity of user-installed software prior to execution to reduce the likelihood of executing malicious code or code that contains errors from unauthorized modifications. Organizations consider the practicality of approaches to verifying software

integrity including, for example, availability of checksums of adequate trustworthiness from software developers or vendors.

CODE EXECUTION IN PROTECTED ENVIRONMENTS

organization-defined personnel or roles
organization-defined personnel or roles
name: SI-7 (13)

statement

Allow execution of binary or machine-executable code only in confined physical or virtual machine environments and with the explicit approval of when such code is:

item
name: SI-7 (13)(a)

Obtained from sources with limited or no warranty; and/or

item
name: SI-7 (13)(b)

Without the provision of source code.

guidance

This control enhancement applies to all sources of binary or machine-executable code including, for example, commercial software and firmware and open source software.

BINARY OR MACHINE EXECUTABLE CODE

name: SI-7 (14)

statement

item
name: SI-7 (14)(a)

Prohibit the use of binary or machine-executable code from sources with limited or no warranty and without the provision of source code; and

item
name: SI-7 (14)(b)

Provide exceptions to the source code requirement only for compelling mission or operational requirements and with the approval of the authorizing official.

guidance

This control enhancement applies to all sources of binary or machine-executable code including, for example, commercial software and firmware and open source software. Organizations assess

software products without accompanying source code from sources with limited or no warranty for potential security impacts. The assessments address the fact that these types of software products may be difficult to review, repair, or extend, given that organizations, in most cases, do not have access to the original source code. In addition, there may be no owners who could make such repairs on behalf of organizations.

CODE AUTHENTICATION

organization-defined software or firmware components
organization-defined software or firmware components
name: SI-7 (15)

statement

Implement cryptographic mechanisms to authenticate prior to installation.

guidance

Cryptographic authentication includes, for example, verifying that software or firmware components have been digitally signed using certificates recognized and approved by organizations. Code signing is an effective method to protect against malicious code.

TIME LIMIT ON PROCESS EXECUTION WITHOUT SUPERVISION

organization-defined time-period
organization-defined time-period
name: SI-7 (16)

statement

Prohibit processes from executing without supervision for more than .

guidance

This control enhancement addresses processes for which typical or normal execution periods can be determined and situations in which organizations exceed such periods. Supervision includes, for example, timers on operating systems, automated responses, or manual oversight and response when system process anomalies occur.
None

References

FIPS Publication 140-2
NIST Special Publication 800-70
NIST Special Publication 800-147

SPAM PROTECTION
name: SI-8

statement

item
name: SI-8a.

Employ spam protection mechanisms at system entry and exit points to detect and act on unsolicited messages; and

item
name: SI-8b.

Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

guidance

System entry and exit points include, for example, firewalls, remote-access servers, electronic mail servers, web servers, proxy servers, workstations, notebook computers, and mobile devices. Spam can be transported by different means including, for example, electronic mail, electronic mail attachments, and web accesses. Spam protection mechanisms include, for example, signature definitions.

CENTRAL MANAGEMENT
name: SI-8 (1)

statement

Centrally manage spam protection mechanisms.

guidance

Central management is the organization-wide management and implementation of spam protection mechanisms. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed spam protection controls.

AUTOMATIC UPDATES
name: SI-8 (2)

statement

Automatically update spam protection mechanisms.

guidance

None.

None

CONTINUOUS LEARNING CAPABILITY

name: SI-8 (3)

statement

Implement spam protection mechanisms with a learning capability to more effectively identify legitimate communications traffic.

guidance

Learning mechanisms include, for example, Bayesian filters that respond to user inputs identifying specific traffic as spam or legitimate by updating algorithm parameters and thereby more accurately separating types of traffic.
None

References

NIST Special Publication 800-45

INFORMATION INPUT RESTRICTIONS

name: SI-9

statement

Incorporated into AC-2, AC-3, AC-5, AC-6.

INFORMATION INPUT VALIDATION

organization-defined information inputs
organization-defined information inputs
name: SI-10

statement

Check the validity of .

guidance

Checking the valid syntax and semantics of system inputs including, for example, character set, length, numerical range, and acceptable values, verifies that inputs match specified definitions for format and content. Software applications typically follow well-defined protocols that use structured messages (i.e., commands or queries) to communicate between software modules or system components. Structured messages can contain raw or unstructured data interspersed with metadata or control information. If software applications use attacker-supplied inputs to construct structured messages without properly encoding such messages, then the

attacker could insert malicious commands or special characters that can cause the data to be interpreted as control information or metadata. Consequently, the module or component that receives the corrupted output will perform the wrong operations or otherwise interpret the data incorrectly. Prescreening inputs prior to passing to interpreters prevents the content from being unintentionally interpreted as commands. Input validation ensures accurate and correct inputs and prevent attacks such as cross-site scripting and a variety of injection attacks.
None

MANUAL OVERRIDE CAPABILITY

organization-defined inputs
organization-defined inputs

organization-defined authorized individuals
organization-defined authorized individuals
name: SI-10 (1)

statement

item
name: SI-10 (1)(a)

Provide a manual override capability for input validation of ;

item
name: SI-10 (1)(b)

Restrict the use of the manual override capability to only ; and

item
name: SI-10 (1)(c)

Audit the use of the manual override capability.

guidance

In certain situations, for example, during events that are defined in organizational contingency plans, a manual override capability for input validation may be needed. Such manual overrides are used only in limited circumstances and with the inputs defined by the organization.

REVIEW AND RESOLVE ERRORS

organization-defined time-period
organization-defined time-period
name: SI-10 (2)

statement

Review and resolve input validation errors within .

guidance

Resolution of input validation errors includes, for example, correcting systemic causes of errors and resubmitting transactions with corrected input.
None

PREDICTABLE BEHAVIOR

name: SI-10 (3)

statement

Verify that the system behaves in a predictable and documented manner when invalid inputs are received.

guidance

A common vulnerability in organizational systems is unpredictable behavior when invalid inputs are received. This control enhancement ensures that there is predictable behavior in the face of invalid inputs by specifying system responses that facilitate transitioning the system to known states without adverse, unintended side effects. The invalid inputs are those inputs related to the information inputs defined by the organization in the base control.
None

TIMING INTERACTIONS

name: SI-10 (4)

statement

Account for timing interactions among system components in determining appropriate responses for invalid inputs.

guidance

In addressing invalid system inputs received across protocol interfaces, timing interactions become relevant, where one protocol needs to consider the impact of the error response on other protocols within the protocol stack. For example, 802.11 standard wireless network protocols do not interact well with Transmission Control Protocols (TCP) when packets are dropped (which could be due to invalid packet input). TCP assumes packet losses are due to congestion, while packets lost over 802.11 links are typically dropped due to collisions or noise on the link. If TCP makes a congestion response, it takes the wrong action in response to a collision event. Adversaries may be able to use what appears to be acceptable individual behaviors of the protocols in concert to achieve adverse effects through suitable construction of invalid input.
None

RESTRICT INPUTS TO TRUSTED SOURCES AND APPROVED FORMATS

organization-defined trusted sources
organization-defined trusted sources

organization-defined formats
organization-defined formats
name: SI-10 (5)

statement

Restrict the use of information inputs to and/or .

guidance

This control enhancement applies the concept of whitelisting to information inputs. Specifying known trusted sources for information inputs and acceptable formats for such inputs can reduce the probability of malicious activity.

ERROR HANDLING

organization-defined personnel or roles
organization-defined personnel or roles
name: SI-11

statement

item
name: SI-11a.

Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited; and

item
name: SI-11b.

Reveal error messages only to .

guidance

Organizations consider the structure and the content of error messages. The extent to which systems can handle error conditions is guided and informed by organizational policy and operational requirements. Exploitable information includes, for example, erroneous logon attempts with passwords entered by mistake as the username; mission/business information

that can be derived from, if not stated explicitly by, the information recorded; and personally identifiable information such as account numbers, social security numbers, and credit card numbers. In addition, error messages may provide a covert channel for transmitting information.

INFORMATION MANAGEMENT AND RETENTION

name: SI-12

statement

Manage and retain information within the system and information output from the system in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, guidelines and operational requirements.

guidance

Information management and retention requirements cover the full life cycle of information, in some cases extending beyond system disposal. Information to be retained may also include policies, procedures, plans, and other types of administrative information. The National Archives and Records Administration provides guidance on records retention.
All XX-1 Controls

LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS

organization-defined elements
organization-defined elements

name: SI-12 (1)

statement

Limit personally identifiable information being processed in the information life cycle to the identified in the privacy risk assessment.

guidance

Limiting the use of personally identifiable information throughout the information life cycle when such information is not needed for operational purposes helps reduce the level of privacy risk created by a system. The information life cycle includes information creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposition.
None

MINIMIZE PERSONALLY IDENTIFIABLE INFORMATION IN TESTING, TRAINING, AND RESEARCH

organization-defined techniques
organization-defined techniques

name: SI-12 (2)

statement

Use to minimize the use of personally identifiable information for research, testing, or training, in accordance with the privacy risk assessment.

guidance

Organizations can minimize the risk to an individual#s privacy by using techniques such as de-identification or synthetic data. Limiting the use of personally identifiable information throughout the information life cycle when such information is not needed for research, testing, or training helps reduce the level of privacy risk created by a system.

PREDICTABLE FAILURE PREVENTION

organization-defined system components
organization-defined system components

organization-defined MTTF substitution criteria
organization-defined MTTF substitution criteria
name: SI-13

statement

item
name: SI-13a.

Determine mean time to failure (MTTF) for in specific environments of operation; and

item
name: SI-13b.

Provide substitute system components and a means to exchange active and standby components at .

guidance

While MTTF is primarily a reliability issue, this control addresses potential failures of system components that provide security capability. Failure rates reflect installation-specific consideration, not industry-average. Organizations define the criteria for substitution of system components based on the MTTF value with consideration for resulting potential harm from component failures. Transfer of responsibilities between active and standby components does not compromise safety, operational readiness, or security capability. This includes, for example, preservation of system state variables. Standby components remain available at all times except for maintenance issues or recovery failures in progress.

TRANSFERRING COMPONENT RESPONSIBILITIES

organization-defined fraction or percentage
organization-defined fraction or percentage
name: SI-13 (1)

statement

Takes system components out of service by transferring component responsibilities to substitute components no later than of mean time to failure.

guidance

None.
None

TIME LIMIT ON PROCESS EXECUTION WITHOUT SUPERVISION

name: SI-13 (2)
SI-7(16)

statement

Incorporated into SI-7(16).

MANUAL TRANSFER BETWEEN COMPONENTS

organization-defined percentage
organization-defined percentage
name: SI-13 (3)

statement

Manually initiate transfers between active and standby system components when the use of the active component reaches of the mean time to failure.

guidance

For example, if the MTTF for a system component is one hundred days and the organization-defined percentage is ninety percent, the manual transfer would occur after ninety days.
None

STANDBY COMPONENT INSTALLATION AND NOTIFICATION

organization-defined time-period
organization-defined time-period

organization-defined alarm
organization-defined alarm

organization-defined action
organization-defined action
name: SI-13 (4)

statement

If system component failures are detected:

item
name: SI-13 (4)(a)

Ensure that the standby components are successfully and transparently installed within ; and

item
name: SI-13 (4)(b)

[Selection (one or more): Activate ; Automatically shut down the system;].

guidance

Automatic or manual transfer of components from standby to active mode can occur, for example, upon detection of component failures.
None

FAILOVER CAPABILITY

organization-defined failover capability
organization-defined failover capability
name: SI-13 (5)

statement

Provide [Selection: real-time; near real-time] for the system.

guidance

Failover refers to the automatic switchover to an alternate system upon the failure of the primary system. Failover capability includes, for example, incorporating mirrored system operations at alternate processing sites or periodic data mirroring at regular intervals defined by recovery time-periods of organizations.

NON-PERSISTENCE

organization-defined system components and services
organization-defined system components and services

organization-defined frequency
organization-defined frequency
name: SI-14

statement

Implement non-persistent that are initiated in a known state and terminated [Selection (one or more): upon end of session of use; periodically at].

guidance

This control mitigates risk from advanced persistent threats (APTs) by significantly reducing the targeting capability of adversaries (i.e., window of opportunity and available attack surface) to initiate and complete attacks. By implementing the concept of non-persistence for selected system components, organizations can provide a known state computing resource for a specific time-period that does not give adversaries sufficient time on target to exploit vulnerabilities in organizational systems and the environments in which those systems operate. Since the APT is a high-end, sophisticated threat regarding capability, intent, and targeting, organizations assume that over an extended period, a percentage of attacks will be successful. Non-persistent system components and services are activated as required using protected information and terminated periodically or at the end of sessions. Non-persistence increases the work factor of adversaries in attempting to compromise or breach organizational systems. Non-persistence can be achieved by refreshing system components, for example, by periodically re-imaging components or by using a variety of common virtualization techniques. Non-persistent services can be implemented using virtualization techniques as part of virtual machines or as new instances of processes on physical machines (either persistent or non-persistent). The benefit of periodic refreshes of system components and services is that it does not require organizations to first determine whether compromises of components or services have occurred (something that may often be difficult to determine). The refresh of selected system components and services occurs with sufficient frequency to prevent the spread or intended impact of attacks, but not with such frequency that it makes the system unstable. Refreshes of critical components and services may be done periodically to hinder the ability of adversaries to exploit optimum windows of vulnerabilities.

REFRESH FROM TRUSTED SOURCES

organization-defined trusted sources
organization-defined trusted sources
name: SI-14 (1)

statement

Obtain software and data employed during system component and service refreshes from .

guidance

Trusted sources include, for example, software and data from write-once, read-only media or from selected off-line secure storage facilities.
None

INFORMATION OUTPUT FILTERING

organization-defined software programs and/or applications
organization-defined software programs and/or applications
name: SI-15

statement

Validate information output from to ensure that the information is consistent with the expected content.

guidance

Certain types of attacks, including for example, SQL injections, produce output results that are unexpected or inconsistent with the output results that would normally be expected from software programs or applications. This control enhancement focuses on detecting extraneous content, preventing such extraneous content from being displayed, and then alerting monitoring tools that anomalous behavior has been discovered.

LIMIT PERSONALLY IDENTIFIABLE INFORMATION DISSEMINATION

organization-defined elements
organization-defined elements
name: SI-15 (1)

statement

Limit the dissemination of personally identifiable information to identified in the privacy risk assessment and consistent with authorized purposes.

guidance

Preventing the sharing of personally identifiable information outside of explicitly determined elements helps mitigate privacy risks that may arise from using such information to detect anomalous system behavior. Organizations weigh the risks created by using personally identifiable information for information output filtering (as either signature or heuristic information) against the security risks they help mitigate and the established privacy posture in the privacy program plan.

MEMORY PROTECTION

organization-defined security safeguards
organization-defined security safeguards
name: SI-16

statement

Implement to protect the system memory from unauthorized code execution.

guidance

Some adversaries launch attacks with the intent of executing code in non-executable regions of memory or in memory locations that are prohibited. Security safeguards employed to protect memory include, for example, data execution prevention and address space layout randomization. Data execution prevention safeguards can either be hardware-enforced or software-enforced with hardware enforcement providing the greater strength of mechanism.

FAIL-SAFE PROCEDURES

organization-defined fail-safe procedures
organization-defined fail-safe procedures

organization-defined failure conditions occur
organization-defined failure conditions occur
name: SI-17

statement

Implement when .

guidance

Failure conditions include, for example, loss of communications among critical system components or between system components and operational facilities. Fail-safe procedures include, for example, alerting operator personnel and providing specific instructions on subsequent steps to take. These steps include, for example, doing nothing, reestablishing system settings, shutting down processes, restarting the system, or contacting designated organizational personnel.

INFORMATION DISPOSAL

organization-defined techniques or methods
organization-defined techniques or methods

name: SI-18

statement

Use to dispose of, destroy, or erase information.

guidance

Disposal or destruction of information applies to originals as well as copies and archived records, including system logs that may contain personally identifiable information.

DATA QUALITY OPERATIONS

organization-defined frequency
organization-defined frequency
name: SI-19

statement

item
name: SI-19a.

Upon collection or creation of personally identifiable information, check for the accuracy, relevance, timeliness, impact, completeness, and de-identification of that information across the information life cycle; and

item
name: SI-19b.

Check for and correct as necessary and across the information life cycle:

item
name: SI-19b.1.

Inaccurate or outdated personally identifiable information;

item
name: SI-19b.2.

Personally identifiable information of incorrectly determined impact; or

item
name: SI-19b.3.

Incorrectly de-identified personally identifiable information.

guidance

The information life cycle includes information creation, collection, use, processing, storage, maintenance, dissemination, disclosure, disposition.

UPDATING AND CORRECTING PERSONALLY IDENTIFIABLE INFORMATION

name: SI-19 (1)

statement

Employ technical controls to correct personally identifiable information used in organizational programs and systems that is inaccurate or outdated, incorrectly determined regarding impact, or incorrectly de-identified.

guidance

Use of controls to improve data quality may inadvertently create privacy risks. Automated controls may connect to external or otherwise unrelated systems, and the matching of records between these systems may create linkages with unintended consequences. Organizations assess and document these risks in their privacy impact assessment and make determinations that are in alignment with their privacy program plan.

DATA TAGS

name: SI-19 (2)

statement

Employ data tags to automate tracking of personally identifiable information across the information life cycle within organizational systems.

guidance

Data tags that contain information about retention dates, usage or disclosure policies, or other information pertaining to the management of personally identifiable information can support the use of automation tools to enforce relevant data management policies.

None

PERSONALLY IDENTIFIABLE INFORMATION COLLECTION

name: SI-19 (3)

statement

Collect personally identifiable information directly from the individual.

guidance

Organizations take reasonable steps to confirm the accuracy and relevance of personally identifiable information. These steps may include, for example, editing and validating addresses as they are collected or entered into systems using automated address verification look-up application programming interfaces. The types of measures taken to protect data quality are

based on the nature and context of the personally identifiable information, how it is to be used, and how it was obtained. Measures taken to validate the accuracy of personally identifiable information used to make determinations about the rights, benefits, or privileges of individuals under federal programs may be more comprehensive than those used to validate less sensitive personally identifiable information. Additional steps may be necessary to validate personally identifiable information that is obtained from sources other than individuals or the authorized representatives of individuals.
None

DE-IDENTIFICATION

name: SI-20

statement

Remove personally identifiable information from datasets.

guidance

Many datasets contain information about individuals that can be used to distinguish or trace an individual#s identity, such as name, social security number, date and place of birth, mother#s maiden name, or biometric records. Datasets may also contain other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. Personally identifiable information is removed from datasets by trained individuals when such information is not (or no longer) necessary to satisfy the requirements envisioned for the data. For example, if the dataset is only used to produce aggregate statistics, the identifiers that are not needed for producing those statistics are removed. Removing identifiers improves privacy protection, since information that is removed cannot be inadvertently disclosed or improperly used.

COLLECTION

name: SI-20 (1)

statement

De-identify the dataset upon collection by not collecting personally identifiable information.

guidance

If a data source contains personally identifiable information but the information will not be used, the dataset can be de-identified upon creation by simply not collecting the data elements containing the personally identifiable information. For example, if an organization does not intend to use the social security number of an applicant, then application forms do not ask for a social security number.
None

ARCHIVING

name: SI-20 (2)

statement

Refrain from archiving personally identifiable information elements if those elements in a dataset will not be needed after the dataset is archived.

guidance

Datasets can be archived for many reasons. The envisioned purposes for the archived dataset are specified and if personally identifiable information elements are not required, the elements are not archived. For example, social security numbers may have been collected for record linkage, but the archived dataset may include the required elements from the linked records. In this case, it is not necessary to archive the social security numbers.
None

RELEASE

name: SI-20 (3)

statement

Remove personally identifiable information elements from a dataset prior to its release if those elements in the dataset do not need to be part of the data release.

guidance

Prior to releasing a dataset, a data custodian considers the intended uses of the released dataset and determines if it is necessary to release personally identifiable information. If it is not necessary, the personally identifiable information can be removed using de-identification techniques.
None

REMOVAL, MASKING, ENCRYPTION, HASHING, OR REPLACEMENT OF DIRECT IDENTIFIERS

name: SI-20 (4)

statement

Remove, mask, encrypt, hash, or replace direct identifiers in a dataset.

guidance

There are many possible processes for removing direct identifiers from a dataset. Columns in a dataset that contain a direct identifier can be removed. In masking, the direct identifier is transformed into a repeating character, for example, XXXXXX or 999999. Identifiers can be encrypted or hashed, so that the linked records remain linked. In the case of encryption or hashing, algorithms are employed that require the use of a key, including, for example, the

Advanced Encryption Standard or a Hash-based Message Authentication Code. Implementations may use the same key for all identifiers or a different key for each identifier. Using a different key for each identifier provides for a higher degree of security and privacy. Identifiers can alternatively be replaced with a keyword, including for example, transforming #George Washington# to #PATIENT,# or replaced with a realistic surrogate value, including for example, transforming #George Washington# to #Abraham Polk.#
None

STATISTICAL DISCLOSURE CONTROL

name: SI-20 (5)

statement

Manipulate numerical data, contingency tables, and statistical findings so that no person or organization is identifiable in the results of the analysis.

guidance

Many types of statistical analyses can result in the disclosure of information about individuals even if only summary information is provided. For example, if a school publishes a monthly table with the number of minority students, and in January the school reports that it has 10-19 such students, but in March it reports that it has 20-29 such students, then it can be inferred that the student who enrolled in February was a minority.
None

DIFFERENTIAL PRIVACY

name: SI-20 (6)

statement

Prevent disclosure of personally identifiable information by adding non-deterministic noise to the results of mathematical operations before the results are reported.

guidance

The mathematical definition for differential privacy holds that the result of a dataset analysis should be approximately the same before and after the addition or removal of a single data record (which is assumed to be the data from a single individual). In its most basic form, differential privacy applies only to online query systems. However, it can also be used to produce machine-learning statistical classifiers and synthetic data. Differential privacy comes at the cost of decreased accuracy of results, forcing organizations to quantify the trade-off between privacy protection and the overall accuracy, usefulness, and utility of the de-identified dataset. Non-deterministic noise can include, for example, adding small random values to the results of mathematical operations in dataset analysis.
None

VALIDATED SOFTWARE

name: SI-20 (7)

statement

Perform de-identification using validated algorithms and software that is validated to implement the algorithms.

guidance

Algorithms that appear to remove personally identifiable information from a dataset may in fact leave information that is personally identifiable or data that are re-identifiable. Software that is claimed to implement a validated algorithm may contain bugs or may implement a different algorithm. Software may de-identify one type of data, for example, integers, but not another type of data, for example, floating point numbers. For these reasons, de-identification is performed using algorithms and software that are validated.
None

MOTIVATED INTRUDER

name: SI-20 (8)

statement

Perform a motivated intruder test on the de-identified dataset to determine if the identified data remains or if the de-identified data can be re-identified.

guidance

A motivated intruder test is a test in which a person or group takes a data release and specified resources and attempts to re-identify one or more individuals in the de-identified dataset. Such tests specify the amount of inside knowledge, financial resources, computational resources, data, and skills that intruders have at their disposal to conduct the tests. A motivated intruder test can identify if de-identification is insufficient. It can also be a useful diagnostic tool to assess if de-identification is likely to be sufficient; however, the test alone cannot prove that de-identification is sufficient.
None