NIST Special Publication 800-53
Revision 4

Security and Privacy Controls for Federal Information Systems and Organizations Appendix F

NOTE: THIS DOCUMENT PROVIDES A MARKUP OF CHANGES MADE TO SP 800-53, REVISION 3 APPENDIX F TO PRODUCE REVISION 4 APPENDIX F. ALTHOUGH A REVIEW WAS MADE TO CONFIRM THE ACCURACY OF THE WORD PROCESSING COMPARISON FUNCTION USED TO IDENTIFY THE CHANGES, THE CHANGES IN SOME CASES WERE CONSIDERABLE, AND THE MARKUP VERSION OF THE CHANGES MAY NOT BE EXACT. AS SUCH, THE MARKUP VERSION SHOULD BE VIEWED AS A GENERAL GUIDE TO THE CHANGES MADE TO REVISION 3 TO PRODUCE REVISION 4 OF SP 800-53. ANY DISCREPANCIES NOTED BETWEEN THE MARKUP AND CLEAN COPIES OF SP 800-53, REVISION 4, PLEASE DEFER TO THE CLEAN COPY FOR THE OFFICIAL VERSION OF CHANGES.

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

Formatted: Font: 28 pt, Bold

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

http://dx.doi.org/10.6028/NIST.SP.800-53r4

Formatted: Font: 11 pt

MARKUP COPY

From: Revision 3 – August 2009
To: Revision 4 – April 2013
INCLUDES UPDATES AS OF 05-07-2013

April 2013
INCLUDES UPDATES AS OF 05-07-2013: PAGE XVII

U.S. Department of Commerce
Rebecca M. Blank, Acting Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Under Secretary of Commerce for Standards and Technology and Director

APPENDIX F

SECURITY CONTROL CATALOG

SECURITY CONTROLS, ENHANCEMENTS, AND SUPPLEMENTAL GUIDANCE

The catalog of security controls in this appendix provides a range of safeguards and countermeasures for organizations and information systems.[1] The security controls have been designed to facilitate compliance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines.[2] The organization of the security control catalog, the structure of the security controls, and the concept of allocating security controls and control enhancements to the initial baselines in Appendix D are described in Chapter Two. The security controls in the catalog with few exceptions, have been designed to be policy- and technology-neutral. This means that security controls and control enhancements focus on the fundamental safeguards and countermeasures necessary to protect information during processing, while in storage, and during transmission. Therefore, it is beyond the scope of this publication to provide guidance on the application of security controls to specific technologies, communities of interest, environments of operation, or missions/business functions. These areas are addressed by the use of the tailoring process described in Chapter Three and the development of overlays described in Appendix I.

In the few cases where specific technologies are called out in security controls (e.g., mobile, PKI, wireless, VOIP), organizations are cautioned that the need to provide adequate security goes well beyond the requirements in a single control associated with a particular technology. Many of the needed safeguards/countermeasures are obtained from the other security controls in the catalog allocated to the initial control baselines as the starting point for the development of security plans and overlays using the tailoring process. In addition to the organization-driven development of specialized security plans and overlays, NIST Special Publications and Interagency Reports may provide guidance on recommended security controls for specific technologies and sector-specific applications (e.g., Smart Grid, healthcare, Industrial Control Systems, and mobile).

Employing a policy- and technology-neutral security control catalog has the following benefits:

- It encourages organizations to focus on the *security capabilities* required for mission/business success and the protection of information, irrespective of the information technologies that are employed in organizational information systems;

[1] An online version of the catalog of security controls is also available at http://web.nvd.nist.gov/view/800-53/home.

[2] Compliance necessitates organizations executing *due diligence* with regard to information security and risk management. Information security due diligence includes using all appropriate information as part of an organization-wide risk management program to effectively use the tailoring guidance and inherent flexibility in NIST publications so that the selected security controls documented in organizational security plans meet the specific mission and business requirements of organizations. Using the risk management tools and techniques that are available to organizations is essential in developing, implementing, and maintaining the safeguards and countermeasures with the necessary and sufficient strength of mechanism to address the current threats to organizational operations and assets, individuals, other organizations, and the Nation. Employing effective risk-based processes, procedures, and technologies will help ensure that all federal information systems and organizations have the necessary resilience to support ongoing federal responsibilities, critical infrastructure applications, and continuity of government.

- It encourages organizations to analyze each security control for its applicability to specific technologies, environments of operation, missions/business functions, and communities of interest; and
- It encourages organizations to specify security policies as part of the tailoring process for security controls that have variable parameters.

For example, organizations using smart phones, tablets, or other types of mobile devices would start the tailoring process by assuming that *all* security controls and control enhancements in the appropriate baseline (low, moderate, or high) are needed. The tailoring process may result in certain security controls being eliminated for a variety of reasons, including, for example, the inability of the technology to support the implementation of the control. However, the elimination of such controls without understanding the potential adverse impacts to organizational missions and business functions can significantly increase information security risk and should be carefully analyzed. This type of analysis is essential in order for organizations to make effective risk-based decisions including the selection of appropriate compensating security controls, when considering the use of these emerging mobile devices and technologies. The specialization of security plans using the tailoring guidance and overlays, together with a comprehensive set of technology- and policy-neutral security controls, promotes cost-effective, risk-based information security for organizations—in any sector, for any technology, and in any operating environment.

The security controls in the catalog are expected to change over time, as controls are withdrawn, revised, and added. In order to maintain stability in security plans and automated tools supporting the implementation of Special Publication 800-53, security controls will not be renumbered each time a control is withdrawn. Rather, notations of security controls that have been withdrawn are maintained in the catalog for historical purposes. Security controls are withdrawn for a variety of reasons including, for example: the security capability provided by the withdrawn control has been incorporated into another control; the security capability provided by the withdrawn control is redundant to an existing control; or the security control is deemed to be no longer necessary.

Deleted: NIST

Deleted: and control enhancements

Deleted: or enhancement

Deleted: Notations

Deleted: and controls enhancements

Deleted: will be

There may, on occasion, be repetition in requirements that appear in the security controls and control enhancements that are part of the security control catalog. This repetition in requirements is intended to reinforce the security requirements from the perspective of multiple controls and/or enhancements. For example, the requirement for strong identification and authentication when conducting remote maintenance activities appears in the MA family in the specific context of systems maintenance activities conducted by organizations. The identification and authentication requirement also appears in a more general context in the IA family. While these requirements appear to be redundant (i.e., overlapping), they are, in fact, mutually reinforcing and not intended to require additional effort on the part of organizations in the development and implementation of security programs.

Implementation Tip

New security controls and control enhancements will be developed on a regular basis using state-of-the-practice information from national-level threat and vulnerability databases as well as information on the tactics, techniques, and procedures employed by adversaries in launching cyber attacks. The proposed modifications to security controls and security control baselines will be carefully weighed during each revision cycle, considering the desire for stability of the security control catalog and the need to respond to changing threats, vulnerabilities, attack methods, and information technologies. The overall objective is to raise the basic level of information security over time. Organizations may choose to develop new security controls when there is a specific security capability required and the appropriate controls are not available in Appendices F or G.

SECURITY CONTROL CLASS DESIGNATIONS

MANAGEMENT, OPERATIONAL, AND TECHNICAL REFERENCES

Because many security controls within the security control families in Appendix F have various combinations of *management*, *operational*, and *technical* properties, the specific class designations have been removed from the security control families. Organizations may still find it useful to apply such designations to individual security controls and control enhancements or to individual sections within a particular control/enhancement. Organizations may find it beneficial to employ class designations as a way to group or refer to security controls. The class designations may also help organizations with the process of allocating security controls and control enhancements to: (i) responsible parties or information systems (e.g., as common or hybrid controls); (ii) specific roles; and/or (iii) specific components of a system. For example, organizations may determine that the responsibility for system-specific controls they have placed in the management class belong to the information system owner, controls placed in the operational class belong to the Information System Security Officer (ISSO), and controls placed in the technical class belong to one or more system administrators. This example is provided to illustrate the potential usefulness of designating classes for controls and/or control enhancements; it is not meant to suggest or require additional tasks for organizations.

CAUTIONARY NOTE

DEVELOPMENT OF SYSTEMS, COMPONENTS, AND SERVICES

With the renewed emphasis on trustworthy information systems and supply chain security, it is essential that organizations have the capability to express their information security requirements with clarity and specificity in order to engage the information technology industry and obtain the systems, components, and services necessary for mission and business success. To ensure that organizations have such capability, Special Publication 800-53 provides a set of security controls in the System and Services Acquisition family (i.e., SA family) addressing requirements for the development of information systems, information technology products, and information system services. Therefore, many of the controls in the SA family are directed at developers of those systems, components, and services. It is important for organizations to recognize that the scope of the security controls in the SA family includes all system/component/service development and the developers associated with such development whether the development is conducted by internal organizational personnel or by external developers through the contracting/acquisition process. Affected controls include SA-8, SA-10, SA-11, SA-15, SA-16, SA-17, SA-20, and SA-21.

Formatted: Font: (Default) Arial, 11 pt, Font color: Black

Deleted:

Fundamentals of the Catalog

Security controls and control enhancements in Appendices F and G are generally designed to be policy-neutral and technology/implementation-independent. Organizations provide information about security controls and control enhancements in two ways:

- By specifying security control implementation details (e.g., platform dependencies) in the associated security plan for the information system or security program plan for the organization; and
- By establishing specific values in the variable sections of selected security controls through the use of *assignment* and *selection* statements.

Assignment and selection statements provide organizations with the capability to specialize security controls and control enhancements based on organizational security requirements or requirements originating in federal laws, Executive Orders, directives, policies, regulations, standards, or guidelines. Organization-defined parameters used in assignment and selection statements in the basic security controls apply also to all control enhancements associated with those controls. Control enhancements strengthen the fundamental security capability in the base control but are not a substitute for using assignment or selection statements to provide greater specificity to the control. Assignment statements for security controls and control enhancements do not contain minimum or maximum values (e.g., testing contingency plans *at least annually*). Organizations should consult specific federal laws, Executive Orders, directives, regulations, policies, standards, or guidelines as the definitive sources for such information. The absence of minimum and maximum values from the security controls and control enhancements does not obviate the need for organizations to comply with requirements in the controlling source publications.

The first security control in each family (i.e., the dash-1 control) generates requirements for specific policies and procedures that are needed for the effective implementation of the other security controls in the family. Therefore, individual controls and control enhancements in a particular family do not call for the development of such policies and procedures. Supplemental guidance sections of security controls and control enhancements do not contain any requirements or references to FIPS or NIST Special Publications. NIST publications are, however, included in a *references* section for each security control.

In support of the Joint Task Force initiative to develop a unified information security framework for the federal government, security controls and control enhancements for national security systems are included in this appendix. The inclusion of such controls and enhancements is not intended to impose security requirements on organizations that operate national security systems. Rather, organizations can use the security controls and control enhancements on a voluntary basis with the approval of federal officials exercising policy authority over national security systems. In addition, the security control priorities and security control baselines listed in Appendix D and in the priority and baseline allocation summary boxes below each security control in Appendix F, apply to non-national security systems *only* unless otherwise directed by the federal officials with national security policy authority.

Using the Catalog

Organizations employ security controls[3] in federal information systems and the environments in which those systems operate in accordance with FIPS Publication 199, FIPS Publication 200, and NIST Special Publications 800-37 and 800-39. Security categorization of federal information and information systems, as required by FIPS Publication 199, is the first step in the risk management process.[4] Next, organizations select an appropriate set of security controls for their information systems by satisfying the minimum security requirements set forth in FIPS Publication 200. Appendix D includes three security control baselines that are associated with the designated impact levels of information systems as determined during the security categorization process.[5] After baseline selection, organizations tailor the baselines by: (i) identifying/designating common controls; (ii) applying scoping considerations; (iii) selecting compensating controls, if needed; (iv) assigning control parameter values in selection and assignment statements; (v) supplementing the baseline controls with additional controls and control enhancements from the security control catalog; and (vi) providing additional information for control implementation. Organizations can also use the baseline tailoring process with the overlay concept that is described in Section 3.2 and Appendix I. Risk assessments, as described in NIST Special Publication 800-30, guide and inform the security control selection process.[6]

Formatted: Font: 11 pt

CAUTIONARY NOTE

USE OF CRYPTOGRAPHY

If cryptography is required for the protection of information based on the selection of security controls in Appendix F and subsequently implemented by organizational information systems, the cryptographic mechanisms comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. This includes, for NSA-approved cryptography to protect classified information, FIPS-validated cryptography to protect unclassified information, and NSA-approved and FIPS-compliant key management technologies and processes. Security controls SC-12 and SC-13 provide specific information on the selection of appropriate cryptographic mechanisms, including the strength of such mechanisms.

[3] The security controls in Special Publication 800-53 are available online and can be downloaded in various formats from the NIST web site at: http://web.nvd.nist.gov/view/800-53/home.

[4] CNSS Instruction 1253 provides guidance for *security categorization* of national security systems.

[5] CNSS Instruction 1253 provides guidance on *security control baselines* for national security systems and specific tailoring requirements associated with such systems.

[6] There are additional security controls and control enhancements that appear in the catalog that are not used in any of the initial baselines. These additional controls and control enhancements are available to organizations and can be used in the tailoring process to achieve the needed level of protection in accordance with organizational risk assessments.

FAMILY: ACCESS CONTROL

AC-1 ACCESS CONTROL POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

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

b. Reviews and updates the current:

1. Access control policy [*Assignment: organization-defined frequency*]; and

2. Access control procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AC family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

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

Priority and Baseline Allocation:

P1	**LOW** AC-1	**MOD** AC-1	**HIGH** AC-1

AC-2 ACCOUNT MANAGEMENT

Control: The organization:

a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: [*Assignment: organization-defined information system account types*];

b. Assigns account managers for information system accounts;

c. Establishes conditions for group and role membership;

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

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

f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [*Assignment: organization-defined procedures or conditions*];

g. Monitors the use of, information system accounts;

Deleted:
CLASS: TECHNICAL

Deleted: develops,

Deleted: , and reviews/updates

Deleted: *frequency*

Deleted: A formal, documented

Deleted: Formal, documented procedures

Deleted: is intended to produce

Deleted: that are required

Deleted: access control

Deleted: The policy

Deleted: are consistent with

Deleted: policies,

Deleted: Existing organizational

Deleted: additional

Deleted: access control

Deleted: the organization. Access control procedures

Deleted: developed

Deleted: a

Deleted: system, when required.

Deleted: the development of the access control

Deleted: .

Deleted: manages

Deleted: , including:

Deleted: Identifying

Deleted: types (i.e., individual, group,

Deleted: , application, guest/anonymous, and temporary);

Deleted: Establishing

Deleted: Identifying

Deleted: specifying

Deleted: ;¶
<#>Requiring appropriate approvals for requests to establish accounts;¶
<#>Establishing, activating, modifying, disabling, and removing accounts;¶
Specifically authorizing and monitoring the use of guest/anonymous

Deleted: temporary accounts;¶
<#>Notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes;¶
<#>Deactivating: (i) temporary accounts that are no longer required; and (ii) accounts of terminated or transferred users;¶ ...

h. Notifies account managers:

1. When accounts are no longer required;

2. When users are terminated or transferred; and

3. When individual information system usage or need-to-know changes;

i. Authorizes access to the information system based on:

1. A valid access authorization;

2. Intended system usage; and

3. Other attributes as required by the organization or associated missions/business functions;

Deleted: and

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

Deleted: Reviewing

Deleted:].

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

Supplemental Guidance: Information system account types include, for example, individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service. Some of the account management requirements listed above can be implemented by organizational information systems. The identification of authorized users of the information system and the specification of access privileges reflects the requirements in other security controls in the security plan. Users requiring administrative privileges on information system accounts receive additional scrutiny by appropriate organizational personnel (e.g., system owner, mission/business owner, or chief information security officer) responsible for approving such accounts and privileged access. Organizations may choose to define access privileges or other attributes by account, by type of account, or a combination of both. Other attributes required for authorizing access include, for example, restrictions on time-of-day, day-of-week, and point-of-origin. In defining other account attributes, organizations consider system-related requirements (e.g., scheduled maintenance, system upgrades) and mission/business requirements, (e.g., time zone differences, customer requirements, remote access to support travel requirements). Failure to consider these factors could affect information system availability. Temporary and emergency accounts are accounts 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 (e.g., local logon accounts used for special tasks defined by organizations or when network resources are unavailable). Such accounts remain available and are not subject to automatic disabling or removal dates. Conditions for disabling or deactivating accounts include, for example: (i) when shared/group, emergency, or temporary accounts are no longer required; or (ii) when individuals are transferred or terminated. Some types of information system accounts may require specialized training. Related controls: AC-3, AC-4, AC-5, AC-6, AC-10, AC-17, AC-19, AC-20, AU-9, IA-2, IA-4, IA-5, IA-8, CM-5, CM-6, CM-11, MA-3, MA-4, MA-5, PL-4, SC-13.

Deleted: is consistent with

Deleted:

Deleted: organizational officials

Deleted: SA-7

Deleted: , SI-9

Control Enhancements:

(1) *ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT MANAGEMENT*

The organization employs automated mechanisms to support the management of information system accounts.

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

Deleted: The information system automatically terminates

(2) *ACCOUNT MANAGEMENT | REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS*

The information system automatically [*Selection: removes; disables*] temporary and emergency accounts after [*Assignment: organization-defined time period for each type of account*].

Supplemental Guidance: This control enhancement requires the removal of both temporary and emergency accounts automatically after a predefined period of time has elapsed, rather than at the convenience of the systems administrator.

(3) *ACCOUNT MANAGEMENT | DISABLE INACTIVE ACCOUNTS*

The information system automatically disables inactive accounts after [*Assignment: organization-defined time period*].

(4) *ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS*

The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [*Assignment: organization-defined personnel or roles*].

Supplemental Guidance: Related controls: AU-2, AU-12.

(5) *ACCOUNT MANAGEMENT | INACTIVITY LOGOUT*

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

Supplemental Guidance: Related control: SC-23.

(6) *ACCOUNT MANAGEMENT | DYNAMIC PRIVILEGE MANAGEMENT*

The information system implements the following dynamic privilege management capabilities: [*Assignment: organization-defined list of dynamic privilege management capabilities*].

Supplemental Guidance: In contrast to conventional access control approaches which employ static information system accounts and predefined sets of user privileges, dynamic access control approaches (e.g., service-oriented architectures) rely on run time access control decisions facilitated by dynamic privilege management. While user identities may remain relatively constant over time, user privileges may change more frequently based on ongoing mission/business requirements and operational needs of organizations. Dynamic privilege management can include, for example, the 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 refer to mechanisms that change the privileges of users based on dynamic rules as opposed to editing specific user profiles. This type of privilege management includes, for example, automatic adjustments of privileges if users are operating out of their normal work times, or if information systems are under duress or in emergency maintenance situations. This control enhancement also includes the ancillary effects of privilege changes, for example, the potential changes to encryption keys used for communications. Dynamic privilege management can support requirements for information system resiliency. Related control: AC-16.

(7) *ACCOUNT MANAGEMENT | ROLE-BASED SCHEMES*

The organization:

(a) **Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles;**

(b) **Monitors privileged role assignments; and**

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

Supplemental Guidance: Privileged roles are organization-defined roles assigned to individuals that allow those individuals to perform certain security-relevant functions that ordinary users are not authorized to perform. These privileged roles include, for example, key management, account management, network and system administration, database administration, and web administration.

(8) *ACCOUNT MANAGEMENT | DYNAMIC ACCOUNT CREATION*

The information system creates [*Assignment: organization-defined information system accounts*] dynamically.

Supplemental Guidance: Dynamic approaches for creating information system accounts (e.g., as implemented within service-oriented architectures) rely on establishing accounts (identities) at run time for entities that were previously unknown. Organizations plan for dynamic creation

Deleted: termination

Deleted: , as required, appropriate individuals.

Deleted: :¶
Requires

Deleted:

Deleted: *and/*

Deleted:];

Deleted: <#>Determines normal time-of-day and duration usage for information system accounts;¶
<#>Monitors for atypical usage of information system accounts; and¶
<#>Reports atypical usage to designated organizational officials.¶
<#>The information system dynamically manages user privileges and associated access authorizations.¶
Enhancement

Deleted: many

Deleted: architecture implementations

Deleted:

Deleted: the

Deleted: the organization

Deleted: network

Deleted: and

Deleted: Tracks and monitors

Deleted: .

Deleted: Enhancement

of information system accounts by establishing trust relationships and mechanisms with the appropriate authorities to validate related authorizations and privileges.

Supplemental Guidance: Related control: AC-16.

(9) *ACCOUNT MANAGEMENT | RESTRICTIONS ON USE OF SHARED GROUPS / ACCOUNTS*

The organization only permits the use of shared/group accounts that meet [*Assignment: organization-defined conditions for establishing shared/group accounts*].

(10) *ACCOUNT MANAGEMENT | SHARED / GROUP ACCOUNT CREDENTIAL TERMINATION*

The information system terminates shared/group account credentials when members leave the group.

(11) *ACCOUNT MANAGEMENT | USAGE CONDITIONS*

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

Supplemental Guidance: Organizations can describe the specific conditions or circumstances under which information system accounts can be used, for example, by restricting usage to certain days of the week, time of day, or specific durations of time.

(12) *ACCOUNT MANAGEMENT | ACCOUNT MONITORING / ATYPICAL USAGE*

The organization:

(a) Monitors information system accounts for [*Assignment: organization-defined atypical use*]; and

(b) Reports atypical usage of information system accounts to [*Assignment: organization-defined personnel or roles*].

Supplemental Guidance: Atypical usage includes, for example, accessing information systems at certain times of the day and from locations that are not consistent with the normal usage patterns of individuals working in organizations. Related control: CA-7.

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

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

Supplemental Guidance: Users posing a significant risk to organizations include individuals for whom reliable evidence or intelligence indicates either the intention to use authorized access to information systems to cause harm or through whom adversaries will cause harm. Harm includes potential adverse impacts to organizational operations and assets, individuals, other organizations, or the Nation. Close coordination between authorizing officials, information system administrators, and human resource managers is essential in order for timely execution of this control enhancement. Related control: PS-4.

References: None.

Priority and Baseline Allocation:

P1	**LOW** AC-2	**MOD** AC-2 (1) (2) (3) (4)	**HIGH** AC-2 (1) (2) (3) (4) (5) (12) (13)

AC-3 ACCESS ENFORCEMENT

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

Supplemental Guidance: Access control policies (e.g., identity-based policies, role-based policies, attribute-based policies) and access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, domains) in information systems. In addition to enforcing authorized access at the information system level and recognizing that information 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.

Deleted: the

Deleted: policy

Deleted:

Deleted: are employed by organizations to

Deleted: (

Deleted: processes, programs,

Deleted: the

Deleted: system.

Deleted: -

Deleted: are

Deleted: , when necessary,

Deleted: for the organization. Consideration is given to the implementation of an audited, explicit override of automated mechanisms in the event of emergencies or other serious events. If encryption of stored information is employed as an access enforcement mechanism, the cryptography used is FIPS 140-2 (as amended) compliant. For classified information, the cryptography used is largely dependent on the classification level of the information and the clearances of the individuals having access to the information. Mechanisms implemented by AC-3 are configured to enforce authorizations determined by other security controls.

Related controls: AC-2, AC-4, AC-5, AC-6, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AU-9, CM-5, CM-6, CM-11, MA-3, MA-4, MA-5, PE-3.

Control Enhancements:

(1) *ACCESS ENFORCEMENT | RESTRICTED ACCESS TO PRIVILEGED FUNCTIONS*

[Withdrawn: Incorporated into AC-6].

(2) *ACCESS ENFORCEMENT | DUAL AUTHORIZATION*

The information system enforces dual authorization for [*Assignment: organization-defined privileged commands and/or other organization-defined actions*].

Supplemental Guidance: Dual authorization mechanisms require the approval of two authorized individuals in order to execute. Organizations do not require dual authorization mechanisms when immediate responses are necessary to ensure public and environmental safety. Related controls: CP-9, MP-6.

(3) *ACCESS ENFORCEMENT | MANDATORY ACCESS CONTROL*

The information system enforces [*Assignment: organization-defined mandatory access control policies*] over all subjects and objects where the policy specifies that:

(a) The policy is uniformly enforced across all subjects and objects within the boundary of the information system;

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

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

(2) Granting its privileges to other subjects;

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

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

(5) Changing the rules governing access control; and

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

Supplemental Guidance: Mandatory access control as defined in this control enhancement is synonymous with nondiscretionary access control, and is not constrained only to certain historical uses (e.g., implementations using the Bell-LaPadula Model). The above class of mandatory access control policies constrains what actions subjects can take with information obtained from data objects for which they have already been granted access, thus preventing 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 information system has control. Otherwise, the access control policy can be circumvented. This enforcement typically is provided via an implementation that meets the reference monitor concept (see AC-25). The policy is bounded by the information 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 some policy mandate (e.g., law, Executive Order, directive, or regulation) that establishes a policy regarding access to sensitive/classified information and some users of the information system are not authorized access to all sensitive/classified information resident in the information system. This control can operate in conjunction with AC-3 (4). A subject that is 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,

Deleted: SA-7, SC-13, SI-9

Deleted: , based on organizational policies and procedures

Deleted: Enhancement

Deleted: two forms of

Deleted: The organization does

Deleted: employ

Deleted: an

Deleted: response is

Deleted: ***nondiscretionary***

Deleted: *set of users and resources*] where the policy rule set for each policy specifies:

Deleted: <#>Access control information (i.e., attributes) employed by the policy rule set (e.g., position, nationality, age, project, time of day); and¶
<#>Required relationships among the access control information to permit access.¶
Enhancement Supplemental Guidance: Nondiscretionary access control policies that may be implemented by organizations include, for example, Attribute-Based Access Control, Mandatory Access Control, and Originator Controlled Access Control. Nondiscretionary access control policies may be employed by organizations in addition to the employment of discretionary access control policies.¶
For Mandatory Access Control (MAC): Policy establishes coverage over all subjects and objects under its control to ensure that each user receives only that information to which the user is authorized access based on classification of the information, and on user clearance and formal access authorization. The information system assigns appropriate security attributes (e.g., labels/security domains/types) to subjects and objects, and uses these attributes as the basis for MAC decisions. The Bell-LaPadula security model defines allowed access with regard to an organization-defined set of strictly hierarchical security levels as follows: A subject can read an object only if the security level of the subject dominates the security level of the object and a subject can write to an object only if two conditions are met: the security level of the object dominates the security level of the subject, and the security level of the user's clearance dominates the security level of the object (no read up, no write down).¶
For Role-Based Access Control (RBAC): Policy establishes coverage over all users and resources to ensure that access rights are grouped by role name, and access to resources is restricted to users who have been authorized to assume the associated role.¶
<#>The information system enforces a Discretionary Access Control (DAC) policy that:¶

...

while a mandatory access control policy imposes a constraint preventing a subject from passing information to another subject operating at a different sensitivity label, AC-3 (4) permits the subject to pass the information to any subject with the same sensitivity label as the subject. Related controls: AC-25, SC-11.

(4) *ACCESS ENFORCEMENT | DISCRETIONARY ACCESS CONTROL*

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

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

(b) Grant its privileges to other subjects;

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

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

(e) Change the rules governing access control.

Supplemental Guidance: When discretionary access control policies are implemented, subjects are not constrained with regard to what actions they can take with information for which they have already been granted access. Thus, subjects that have been granted access to information are not prevented from passing (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. Thus, 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 information system boundary. Once the information is passed outside of the control of the information system, additional means may be required to 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.

(5) *ACCESS ENFORCEMENT | SECURITY-RELEVANT INFORMATION*

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

Supplemental Guidance: Security-relevant information is any information within information 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 information systems are not performing mission/business-related processing (e.g., the system is off-line for maintenance, troubleshooting, boot-up, shut down). Related control: CM-3.

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

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

(7) *ACCESS ENFORCEMENT | ROLE-BASED ACCESS CONTROL*

The information system enforces a role-based access control policy over defined subjects and objects and controls access based upon [*Assignment: organization-defined roles and users authorized to assume such roles*].

Supplemental Guidance: Role-based access control (RBAC) is an access control policy that restricts information 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 organizational information 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

Deleted: nonoperable

Deleted: Enhancement

Deleted: the

Deleted: system

Deleted: the

Deleted: policy

Deleted: Filtering

Deleted: and

Deleted: key

Deleted: are examples of security-relevant information.

Deleted: nonoperable

Deleted: are states

Deleted: the

Deleted: system is

Deleted: shutdown).

Deleted: The organization encrypts or stores off-line in a secure location [*Assignment: organization-defined user and/or system information*].¶
Enhancement Supplemental Guidance: The use of encryption by the organization reduces the probability of unauthorized disclosure of information and can also detect unauthorized changes to information. Removing information from online storage to offline storage eliminates the possibility of individuals gaining unauthorized access via a network. Related control: MP-4.¶

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.

(8) *ACCESS ENFORCEMENT | REVOCATION OF ACCESS AUTHORIZATIONS*

The information system enforces the revocation of access authorizations resulting from changes to the security attributes of subjects and objects based on [*Assignment: organization-defined rules governing the timing of revocations of access authorizations*].

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

(9) *ACCESS ENFORCEMENT | CONTROLLED RELEASE*

The information system does not release information outside of the established system boundary unless:

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

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

Supplemental Guidance: Information systems can only protect organizational information within the confines of established system boundaries. Additional security safeguards may be needed to ensure that such information is adequately protected once it is passed beyond the established information system boundaries. Examples of information leaving the system boundary include transmitting information to an external information system or printing the information on one of its printers. In cases where the information system is unable to make a determination of the adequacy of the protections provided by entities outside its boundary, as a mitigating control, organizations determine procedurally whether the external information systems are providing adequate security. The means used to determine the adequacy of the security provided by external information systems include, for example, conducting inspections or periodic testing, 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 information systems to employ technical or procedural means to validate the information prior to releasing it to external systems. For example, if the information 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 information 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 (e.g., law, Executive Order, directive, or regulation) that establishes policy regarding access to the information, and that policy applies beyond the realm of a particular information system or organization.

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

The organization employs an audited override of automated access control mechanisms under [*Assignment: organization-defined conditions*].

Supplemental Guidance: Related controls: AU-2, AU-6.

References: None.

Priority and Baseline Allocation:

P1	**LOW** AC-3	**MOD** AC-3	**HIGH** AC-3

AC-4 INFORMATION FLOW ENFORCEMENT

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

Deleted: in accordance with applicable policy.

Supplemental Guidance: Information flow control regulates where information is allowed to travel within an information system and between information 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 information systems representing different security domains with different security policies introduces risk that such transfers violate one or more domain security policies. In such situations, information owners/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: (i) prohibiting information transfers between interconnected systems (i.e., allowing access only); (ii) employing hardware mechanisms to enforce one-way information flows; and (iii) implementing trustworthy regrading mechanisms to reassign security attributes and security labels.

Deleted: A few examples of flow

Deleted: and not passing any web requests to the Internet that are not from the internal web proxy. Information flow control policies and enforcement mechanisms are commonly employed by organizations

Organizations commonly employ information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations (e.g., networks, individuals, and devices) within information systems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Enforcement occurs, for example, in boundary protection devices (e.g., gateways, routers, guards, encrypted tunnels, firewalls) that employ rule sets or establish configuration settings that restrict information system services, provide a packet-filtering capability based on header information, or message-filtering capability based on message content (e.g., implementing key word searches or using document characteristics). Organizations also consider the trustworthiness of filtering/inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement. Control enhancements 3 through 22 primarily address cross-domain solution needs which focus on more advanced filtering techniques, in-depth analysis, and stronger flow enforcement mechanisms implemented in cross-domain products, for example, high-assurance guards. Such capabilities are generally not available in commercial off-the-shelf information technology products. Related controls: AC-3, AC-17, AC-19, AC-21, CM-6, CM-7, SA-8, SC-2, SC-5, SC-7, SC-18.

Deleted:

Deleted: Specific examples of flow control enforcement can be found

Deleted: proxies,

Deleted: , and routers

Deleted: using

Deleted: Mechanisms

Deleted: by AC-4 are configured to enforce authorizations determined by other security controls.

Control Enhancements:

(1) *INFORMATION FLOW ENFORCEMENT | OBJECT SECURITY ATTRIBUTES*

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

Deleted: enforces information flow control using explicit

Deleted: on

Supplemental Guidance: Information flow enforcement mechanisms compare security attributes associated with information (data content and data structure) and source/destination objects, and respond appropriately (e.g., block, quarantine, alert administrator) when the mechanisms encounter information flows not explicitly allowed by information flow policies. For example, an information object labeled *Secret* would be allowed to flow to a destination object labeled *Secret*, but an information object labeled *Top Secret* would not be allowed to flow to a destination object labeled *Secret*. Security attributes can also include, for example, source and destination addresses employed in traffic filter firewalls. Flow enforcement using explicit

Deleted: Enhancement

Deleted: on all

Deleted:),

Deleted: and

Deleted: the

Deleted: policy. Information flow

security attributes can be used, for example, to control the release of certain types of information. Related control: AC-16.

(2) *INFORMATION FLOW ENFORCEMENT | PROCESSING DOMAINS*

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

Deleted: enforces information flow control using

Deleted: (e.g., domain type-enforcement)

Supplemental Guidance: Within information systems, protected processing domains are processing spaces that have controlled interactions with other processing spaces, thus 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, information 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.

(3) *INFORMATION FLOW ENFORCEMENT | DYNAMIC INFORMATION FLOW CONTROL*

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

Deleted: policy that allows

Supplemental Guidance: Organizational policies regarding dynamic information flow control include, for example, allowing or disallowing information flows based on changing conditions or mission/operational considerations. Changing conditions include, for example, changes in organizational risk tolerance due to changes in the immediacy of mission/business needs, changes in the threat environment, and detection of potentially harmful or adverse events. Related control: SI-4.

Deleted: disallows

(4) *INFORMATION FLOW ENFORCEMENT | CONTENT CHECK ENCRYPTED INFORMATION*

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

Deleted: data

Deleted: .

Supplemental Guidance: Related control: SI-4.

(5) *INFORMATION FLOW ENFORCEMENT | EMBEDDED DATA TYPES*

The information system enforces [*Assignment: organization-defined limitations*] on embedding data types within other data types.

Deleted: *the*

Deleted: *of*

Deleted:].

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

(6) *INFORMATION FLOW ENFORCEMENT | METADATA*

The information system enforces information flow control based on [*Assignment: organization-defined metadata*].

Deleted: .

Supplemental Guidance: Metadata is information used to describe the characteristics of data. Metadata can include structural metadata describing data structures (e.g., data format, syntax, and semantics) or descriptive metadata describing data contents (e.g., age, location, telephone number). Enforcing allowed information flows based on metadata enables simpler and more effective flow control. Organizations consider the trustworthiness of metadata with regard to data accuracy (i.e., knowledge that the metadata values are correct with respect to the data), data integrity (i.e., protecting against unauthorized changes to metadata tags), and the binding of metadata to the data payload (i.e., ensuring sufficiently strong binding techniques with appropriate levels of assurance). Related controls: AC-16, SI-7.

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

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

(8) *INFORMATION FLOW ENFORCEMENT | SECURITY POLICY FILTERS*

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

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

(9) *INFORMATION FLOW ENFORCEMENT | HUMAN REVIEWS*

The information system enforces the use of human reviews for [*Assignment: organization-defined information flows*] under the following conditions: [*Assignment: organization-defined conditions*].

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

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

The information system provides the capability for privileged administrators to enable/disable [*Assignment: organization-defined security policy filters*] under the following conditions: [*Assignment: organization-defined conditions*].

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

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

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

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

(12) *INFORMATION FLOW ENFORCEMENT | DATA TYPE IDENTIFIERS*

The information system, when transferring information between different security domains, uses [*Assignment: organization-defined data type identifiers*] to validate data essential for information flow decisions.

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

(13) *INFORMATION FLOW ENFORCEMENT | DECOMPOSITION INTO POLICY-RELEVANT SUBCOMPONENTS*

The information system, when transferring information between different security domains, decomposes information into [Assignment: organization-defined policy-relevant subcomponents] for submission to policy enforcement mechanisms.

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

Deleted: .

Deleted: Enhancement

Deleted: include, for

Deleted: , file type checking filters, structured data filters, unstructured data filters, metadata content filters

Deleted: filters.

Deleted: its

Deleted: virtue of atomic elements that are understandable by an application and indivisible.

Deleted: masses of (usually)

Deleted: that does not have

Deleted: has

Deleted: is not easily readable by a machine.

Deleted: two basic categories

Deleted: a

Deleted: language (i.e

Deleted: review

Deleted:] when the system is not

Deleted: a

Deleted: administrator

Deleted:].

Deleted: a

Deleted: administrator

Deleted: Enhancement

Deleted: the

Deleted: policy, an administrator

Deleted: the

Deleted: mechanism checks

Deleted: the organization

Deleted: identifies information flows b

Deleted: Enhancement

Deleted: specification and usage

Deleted: using

Deleted: naming to reflect type of data and

Deleted: based on file

Deleted: Enhancement

Deleted: include the

Deleted: that are applied

Deleted: transfer to a

Deleted: domain.

Deleted: subject,

Deleted: information

Deleted: . Policy rules for cross domain

(14) *INFORMATION FLOW ENFORCEMENT | SECURITY POLICY FILTER CONSTRAINTS*

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

Supplemental Guidance: Data structure and content restrictions reduce the range of potential malicious and/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: (i) encoding formats for character sets (e.g., Universal Character Set Transformation Formats, American Standard Code for Information Interchange); (ii) restricting character data fields to only contain alpha-numeric characters; (iii) prohibiting special characters; and (iv) validating schema structures.

(15) *INFORMATION FLOW ENFORCEMENT | DETECTION OF UNSANCTIONED INFORMATION*

The information system, when transferring information between different security domains, examines the information for the presence of [*Assignment: organized-defined unsanctioned information*] and prohibits the transfer of such information in accordance with the [*Assignment: organization-defined security policy*].

Supplemental Guidance: Detection of unsanctioned information includes, for example, checking all information to be transferred for malicious code and dirty words. Related control: SI-3.

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

[Withdrawn: Incorporated into AC-4].

(17) *INFORMATION FLOW ENFORCEMENT | DOMAIN AUTHENTICATION*

(18) **The information system uniquely identifies and authenticates source and destination points by [*Selection (one or more): organization, system, application, individual*] for information transfer.**

Supplemental Guidance: Attribution is a critical component of a security concept of operations. The ability to identify source and destination points for information flowing in information 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 information system labels distinguish among systems, organizations, and individuals involved in preparing, sending, receiving, or disseminating information. Related controls: IA-2, IA-3, IA-4, IA-5.

(19) *INFORMATION FLOW ENFORCEMENT | SECURITY ATTRIBUTE BINDING*

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

Supplemental Guidance: Binding techniques implemented by information systems affect the strength of security attribute binding to information. Binding strength and the assurance associated with binding techniques play an important part in the trust organizations have in the information flow enforcement process. The binding techniques affect the number and degree of additional reviews required by organizations. Related controls: AC-16, SC-16.

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

The information system, when transferring information between different security domains, applies the same security policy filtering to metadata as it applies to data payloads.

Supplemental Guidance: This control enhancement requires the validation of metadata and the data to which the metadata applies. Some organizations distinguish between metadata and data payloads (i.e., only the data to which the metadata is bound). Other organizations do not make such distinctions, considering metadata and the data to which the metadata applies as part of the payload. All information (including metadata and the data to which the metadata applies) is subject to filtering and inspection.

(21) *INFORMATION FLOW ENFORCEMENT | APPROVED SOLUTIONS*

The organization employs [*Assignment: organization-defined solutions in approved configurations*] to control the flow of [*Assignment: organization-defined information*] across security domains.

Supplemental Guidance: Organizations define approved solutions and configurations in cross-domain policies and guidance in accordance with the types of information flows across

Deleted: policy filters that constrain data structure and content to

Deleted: *information*

Deleted: *requirements*].

Deleted: Enhancement

Deleted: Constraining file lengths, allowed enumerations, character sets, schemas,

Deleted: other data object attributes reduces the

Deleted: . Examples of constraints include ensuring that: (i) character data fields only contain printable ASCII; (ii) character data fields

Deleted: character data fields do not contain

Deleted: or

Deleted: maximum field sizes and file lengths are enforced based upon organization-defined security policy

Deleted: detects

Deleted: .

Deleted: Enhancement

Deleted: Actions to support this enhancement include:

Deleted:

Deleted: transferred information for malware, implementing dirty word list searches on transferred information, and applying the same protection measures to metadata (e.g., security attributes) that is applied to the information payload.

Deleted: The information system enforces security policies regarding information on interconnected systems.¶
Enhancement Supplemental Guidance: Transferring information between interconnected information systems of differing security policies introduces risk that such transfers …

Deleted: Uniquely

Deleted: domains

Deleted: ;

Deleted: <#>Binds security attributes …

Deleted:

Deleted: an

Deleted: system

Deleted: increases

Deleted: Means to enforce this enhancemen …

Deleted: the

Deleted: resolution

Deleted: between information

Deleted: and

Deleted: between specific system compone …

classification boundaries. The Unified Cross Domain Management Office (UCDMO) provides a baseline listing of approved cross-domain solutions.

(22) *INFORMATION FLOW ENFORCEMENT | PHYSICAL / LOGICAL SEPARATION OF INFORMATION FLOWS*

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

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

(23) *INFORMATION FLOW ENFORCEMENT | ACCESS ONLY*

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

Supplemental Guidance: The information 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.

References: Web: ucdmo.gov.

Deleted: None

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** AC-4	**HIGH** AC-4

AC-5 SEPARATION OF DUTIES

Control: The organization:

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

Deleted: as necessary, to prevent malevolent activity without collusion;

b. Documents separation of duties of individuals; and

c. Defines information system access authorizations to support separation of duties.

Deleted: Implements separation of duties through assigned

Supplemental Guidance: Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example: (i) dividing mission functions and information system support functions among different individuals and/or roles; (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring security personnel administering access control functions do not also administer audit functions. Related controls: AC-3, AC-6, PE-3, PE-4, PS-2.

Deleted: Examples of separation

Deleted: include

Deleted: distinct

Deleted: are divided

Deleted: /

Deleted: different individuals perform

Deleted: systems

Deleted: who administer

Deleted: ; and (iv) different administrator accounts for different roles. Access authorizations defined in this control are implemented by control AC-3.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** AC-5	**HIGH** AC-5

AC-6 LEAST PRIVILEGE

Control: The organization employs 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.

Deleted: concept

Deleted: and

Supplemental Guidance: Organizations employ least privilege for specific duties and information systems. The principle of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions/business functions. Organizations consider the creation of additional processes, roles, and information system accounts as necessary, to achieve least privilege. Organizations also apply least privilege to the development, implementation, and operation of organizational information systems. Related controls: AC-2, AC-3, AC-5, CM-6, CM-7, PL-2.

Deleted: The access authorizations defined in this control are largely implemented by control AC-3. The organization employs the concept of least privilege …rganizations employ least …

Control Enhancements:

(1) *LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS*

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

Deleted: *list of*

Supplemental Guidance: Security functions include, for example, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters. Security-relevant information includes, for example, filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists. Explicitly authorized personnel include, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users. Related controls: AC-17, AC-18, AC-19.

Deleted: Enhancement …upplemental …

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

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

Deleted: *list of …ecurity functions or* …

Supplemental Guidance: This control enhancement limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations implement access control policies such as role-based access control and where a change of role provides the same degree of assurance in the change of access authorizations for both the user and all processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account. Related control: PL-4.

Deleted: Enhancement …upplemental …

(3) *LEAST PRIVILEGE | NETWORK ACCESS TO PRIVILEGED COMMANDS*

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

Supplemental Guidance: Network access is any access across a network connection in lieu of local access (i.e., user being physically present at the device). Related control: AC-17.

(4) *LEAST PRIVILEGE | SEPARATE PROCESSING DOMAINS*

The information system provides separate processing domains to enable finer-grained allocation of user privileges.

Supplemental Guidance: Providing separate processing domains for finer-grained allocation of user privileges includes, for example: (i) using virtualization techniques to allow additional privileges within a virtual machine while restricting privileges to other virtual machines or to the underlying actual machine; (ii) employing hardware and/or software domain separation mechanisms; and (iii) implementing separate physical domains. Related controls: AC-4, SC-3, SC-30, SC-32.

Deleted: Enhancement

Deleted: Employing…roviding separate …

(5) *LEAST PRIVILEGE | PRIVILEGED ACCOUNTS*

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

Deleted: limits authorization to super user…estricts privileged accounts on t …

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

Deleted: Enhancement …upplemental …

system configurations for key security parameters and as otherwise necessary to sufficiently mitigate risk. Related control: CM-6.

Deleted: with regard to

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

The organization prohibits privileged access to the information system by non-organizational users.

Supplemental Guidance: Related control: IA-8.

Deleted: Enhancement

Deleted: A qualified

(7) *LEAST PRIVILEGE | REVIEW OF USER PRIVILEGES*

The organization:

(a) **Reviews [*Assignment: organization-defined frequency*] the privileges assigned to [*Assignment: organization-defined roles or classes of users*] to validate the need for such privileges; and**

(b) **Reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs.**

Deleted: user

Supplemental Guidance: The need for certain assigned user privileges may change over time reflecting changes in organizational missions/business function, environments of operation, technologies, or threat. Periodic review of assigned user privileges is necessary to determine if the rationale for assigning such privileges remains valid. If the need cannot be revalidated, organizations take appropriate corrective actions. Related control: CA-7.

Deleted: be advised by a non-

Deleted: user, if necessary

(8) *LEAST PRIVILEGE | PRIVILEGE LEVELS FOR CODE EXECUTION*

The information system prevents [*Assignment: organization-defined software*] from executing at higher privilege levels than users executing the software.

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

(9) *LEAST PRIVILEGE | AUDITING USE OF PRIVILEGED FUNCTIONS*

The information system audits the execution of privileged functions.

Supplemental Guidance: Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised information 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 (APT). Related control: AU-2.

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

The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

Supplemental Guidance: Privileged functions include, for example, establishing information 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.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** AC-6 (1) (2) (5) (9) (10)	**HIGH** AC-6 (1) (2) (3) (5) (9) (10)

AC-7 UNSUCCESSFUL LOGON ATTEMPTS

Deleted: LOGIN

Control: The information system:

a. Enforces a limit of [*Assignment: organization-defined number*] consecutive invalid logon attempts by a user during a [*Assignment: organization-defined time period*]; and

b. Automatically [*Selection: locks the account/node for an* [*Assignment: organization-defined time period*]; *locks the account/node until released by an administrator; delays next logon prompt according to* [*Assignment: organization-defined delay algorithm*]] when the maximum number of unsuccessful attempts is exceeded.

Supplemental Guidance: This control applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by information systems are usually temporary and automatically release after a predetermined time period established by organizations. If a delay algorithm is selected, organizations may choose to employ different algorithms for different information system components based on the capabilities of those components. Responses to unsuccessful logon attempts may be implemented at both the operating system and the application levels. Related controls: AC-2, AC-9, AC-14, IA-5.

Control Enhancements:

(1) *UNSUCCESSFUL LOGON ATTEMPTS | AUTOMATIC ACCOUNT LOCK*

[Withdrawn: Incorporated into AC-7].

(2) *UNSUCCESSFUL LOGON ATTEMPTS | PURGE / WIPE MOBILE DEVICE*

The information system purges/wipes information from [*Assignment: organization-defined mobile devices*] based on [*Assignment: organization-defined purging/wiping requirements/techniques*] after [*Assignment: organization-defined number*] consecutive, unsuccessful device logon attempts.

Supplemental Guidance: This control enhancement applies only to mobile devices for which a logon occurs (e.g., personal digital assistants, smart phones, tablets). The logon is to the mobile device, not to any one account on the device. Therefore, successful logons to any accounts on mobile devices reset the unsuccessful logon count to zero. Organizations define information to be purged/wiped carefully in order to avoid over purging/wiping which may result in devices becoming unusable. Purging/wiping may be unnecessary if the information on the device is protected with sufficiently strong encryption mechanisms. Related controls: AC-19, MP-5, MP-6, SC-13.

References: None.

Priority and Baseline Allocation:

P2	**LOW** AC-7	**MOD** AC-7	**HIGH** AC-7

AC-8 SYSTEM USE NOTIFICATION

Control: The information system:

a. Displays to users [*Assignment: organization-defined system use notification message or banner*] before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that:

1. Users are accessing a U.S. Government information system;

2. Information system usage may be monitored, recorded, and subject to audit;

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

4. Use of the information system indicates consent to monitoring and recording;

Deleted: access

Deleted: *login*

Deleted: The control applies regardless of whether the login occurs via a local or network connection.

Deleted: the

Deleted: system

Deleted: the organization.

Deleted: the organization

Deleted: chose

Deleted: Response

Deleted: login

Deleted: This control applies to all accesses other than those accesses explicitly identified and documented by the organization in

Deleted: <#>¶

Deleted: The information system automatically locks the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.

Deleted: the device

Deleted: login

Deleted: to the device

Deleted: Enhancement

Deleted: login

Deleted:) and not to mobile devices accessed without a login such as removable media. In certain situations, this enhancement may not apply to mobile devices if the information on the device is encrypted with sufficiently strong encryption mechanisms, making purging unnecessary. The login

Deleted:

Deleted: a

Deleted: login

Deleted: account

Deleted: the

Deleted: device resets

Deleted: login

Deleted: an approved

Deleted: (i) users

Deleted: (ii)

Deleted: (iii) unauthorized

Deleted: (iv) use

b. Retains 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 information system; and

c. For publicly accessible systems:

1. Displays system use information [*Assignment: organization-defined conditions*], before granting further access;

2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and

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

Supplemental Guidance: System use notifications can be implemented using messages or warning banners displayed before individuals log in to information systems. System use notifications are used only for access via logon interfaces with human users and are not required when such human interfaces do not exist. Organizations consider system use notification messages/banners displayed in multiple languages based on specific organizational needs and the demographics of information system users. Organizations also consult with the Office of the General Counsel for legal review and approval of warning banner content.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	**LOW** AC-8	**MOD** AC-8	**HIGH** AC-8

AC-9 PREVIOUS LOGON (ACCESS) NOTIFICATION

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

Supplemental Guidance: This control is applicable to logons to information systems via human user interfaces and logons to systems that occur in other types of architectures (e.g., service-oriented architectures). Related controls: AC-7, PL-4.

Control Enhancements:

(1) *PREVIOUS LOGON NOTIFICATION | UNSUCCESSFUL LOGONS*

The information system notifies the user, upon successful logon/access, of the number of unsuccessful logon/access attempts since the last successful logon/access.

(2) *PREVIOUS LOGON NOTIFICATION | SUCCESSFUL / UNSUCCESSFUL LOGONS*

The information system notifies the user of the number of [*Selection: successful logons/accesses; unsuccessful logon/access attempts; both*] during [*Assignment: organization-defined time period*].

(3) *PREVIOUS LOGON NOTIFICATION | NOTIFICATION OF ACCOUNT CHANGES*

The information system notifies the user of changes to [*Assignment: organization-defined security-related characteristics/parameters of the user's account*] during [*Assignment: organization-defined time period*].

(4) *PREVIOUS LOGON NOTIFICATION | ADDITIONAL LOGON INFORMATION*

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

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

Deleted: (i) displays the

Deleted: when appropriate,

Deleted: (ii) displays

Deleted: (iii) includes in the notice given to public users of the information system, a description of the authorized uses of the system.

Deleted: notification messages

Deleted: in the form of

Deleted: when

Deleted: the

Deleted: system.

Deleted: notification is intended

Deleted: information system

Deleted: that includes an interactive login interface

Deleted: a

Deleted: user

Deleted: is

Deleted: intended to require notification when an interactive interface does

Deleted:),

Deleted: intended

Deleted: cover both traditional

Deleted: general accesses

Deleted: information

Deleted: architectural configurations

Deleted:

Deleted: *logins*

Deleted: *login*

Deleted: *set of*

Deleted: *changes to*

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

AC-10 CONCURRENT SESSION CONTROL

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

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

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P3	**LOW** Not Selected	**MOD** Not Selected	**HIGH** AC-10

AC-11 SESSION LOCK

Control: The information system:

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

b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.

Supplemental Guidance: Session locks are temporary actions taken when users stop work and move away from the immediate vicinity of information systems but do not want to log out because of the temporary nature of their absences. Session locks are implemented where session activities can be determined. This is typically at the operating system level, but can also be at the application level. Session locks are not an acceptable substitute for logging out of information systems, for example, if organizations require users to log out at the end of workdays. Related control: AC-7.

Control Enhancements:

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

The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.

Supplemental Guidance: Publicly viewable images can include static or dynamic images, for example, patterns used with screen savers, photographic images, solid colors, clock, battery life indicator, or a blank screen, with the additional caveat that none of the images convey sensitive information.

References: OMB Memorandum 06-16.

Priority and Baseline Allocation:

Deleted: system account

Deleted: The organization

Deleted: an

Deleted: account

Deleted: ,

Deleted: a given

Deleted: account

Deleted: a

Deleted: user

Deleted: P2

Deleted: A session lock is a

Deleted: action

Deleted: a user stops

Deleted: moves

Deleted: physical

Deleted: the

Deleted: system

Deleted: does

Deleted: the absence. The session lock is

Deleted: at the point

Deleted: activity

Deleted:

Deleted: -

Deleted: may

Deleted: -

Deleted: A session lock is

Deleted: a

Deleted: the

Deleted: system

Deleted: the organization requires

Deleted: the workday

Deleted: session lock mechanism, when activated on a device with a display screen, places a publically viewable pattern onto

Deleted: associated display, hiding what was

P3	**LOW** Not Selected	**MOD** AC-11 (1)	**HIGH** AC-11 (1)

AC-12 SESSION TERMINATION

Deleted: [Withdrawn: Incorporated into SC-10].

Control: The information system automatically terminates a user session after [*Assignment: organization-defined conditions or trigger events requiring session disconnect*].

Supplemental Guidance: This control addresses the termination of user-initiated logical sessions in contrast to SC-10 which addresses the termination of network connections that are associated with communications sessions (i.e., network disconnect). A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organizational information system. Such user sessions can be terminated (and thus terminate user access) without terminating network sessions. Session termination terminates all processes associated with a user's logical session except those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated. Conditions or trigger events requiring automatic session termination can include, for example, organization-defined periods of user inactivity, targeted responses to certain types of incidents, time-of-day restrictions on information system use. Related controls: SC-10, SC-23.

Control Enhancements:

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

The information system:

(a) Provides a logout capability for user-initiated communications sessions whenever authentication is used to gain access to [*Assignment: organization-defined information resources*]; and

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

Supplemental Guidance: Information resources to which users gain access via authentication include, for example, local workstations, databases, and password-protected websites/web-based services. 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, information systems typically send logout messages as final messages prior to terminating sessions.

References: None.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** AC-12	**HIGH** AC-12

AC-13 SUPERVISION AND REVIEW — ACCESS CONTROL

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

AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

Control: The organization:

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

Deleted: specific

b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.

Supplemental Guidance: This control addresses situations in which organizations determine that no identification or authentication is required in organizational information 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 information systems, when individuals use mobile phones to receive calls, or when facsimiles are received. Organizations also identify actions that normally require identification or authentication but may under certain circumstances (e.g., emergencies), allow identification or authentication mechanisms to be bypassed. Such bypasses may occur, for example, via a software-readable physical switch that commands bypass of the logon functionality and is protected from accidental or unmonitored use. This control does not apply to situations where identification and authentication have already occurred and are not repeated, but rather to situations where identification and authentication have not yet occurred. Organizations may decide that there are no user actions that can be performed on organizational information systems without identification and authentication and thus, the values for assignment statements can be *none*. Related controls: CP-2, IA-2.

Control Enhancements: None.

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

References: None.

Priority and Baseline Allocation:

P3	**LOW** AC-14	**MOD** AC-14	**HIGH** AC-14

AC-15 AUTOMATED MARKING

[Withdrawn: Incorporated into MP-3].

AC-16 SECURITY ATTRIBUTES

Control: The organization:

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

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

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

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

Supplemental Guidance: Information is represented internally within information 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. These 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,

Deleted: and

Deleted: is intended for those specific instances where an organization determines

Deleted: and

Deleted: ; it is not, however, mandating that such instances exist

Deleted: given

Deleted: system. The organization

Deleted: and

Deleted: (e.g.,

Deleted: such as http://www.usa.gov).

Deleted: any

Deleted:

Deleted: bypass

Deleted: be

Deleted: login

Deleted:

Deleted: being

Deleted: /or

Deleted: The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission/business objectives.¶

Deleted: P1

Deleted: (1)

Deleted: (1)

Deleted: information system supports and maintains the binding of

Deleted: to

Deleted: .

Deleted: an entity (e.g., subjects

Deleted: objects)

Deleted:

Deleted: are typically associated with or to change the information system state. These attributes may also be associated with passive entities (i.e., objects) that contain or receive information. The association of security attributes to subjects and objects is referred to as *binding* and is typically inclusive of setting the attribute value and the attribute type. Security attributes when bound to data/information, enables the enforcement of information security policies for access control and information flow control, either through organizational processes or information system functions or mechanisms. The content or assigned values of security attributes can directly affect the ability of individuals to access organizational information.

Organizations can define the types of attributes needed for selected information systems to support missions/business functions. There is potentially a wide range of values that can be assigned to any given security attribute. Release markings could include, for example, US only, NATO, or NOFORN (not releasable to foreign nationals). By specifying permitted attribute ranges and values, organizations can ensure that the security attribute values are meaningful and relevant. The term *security labeling* refers to the association of security attributes with subjects and objects represented by internal data structures within organizational information systems, to enable information system-based enforcement of information security policies. Security labels include, for example, access authorizations, data life cycle protection (i.e., encryption and data expiration), nationality, affiliation as contractor, and classification of information in accordance with legal and compliance requirements. The term security marking refers to the association of security attributes with objects in a human-readable form, to enable organizational process-based enforcement of information security policies. The AC-16 base control represents the requirement for user-based attribute association (marking). The enhancements to AC-16 represent additional requirements including information system-based attribute association (labeling). Types of attributes include, for example, classification level for objects and clearance (access authorization) level for subjects. An example of a value for both of these attribute types is *Top Secret*. Related controls: AC-3, AC-4, AC-6, AC-21, AU-2, AU-10, SC-16, MP-3.

Control Enhancements:

(1) *SECURITY ATTRIBUTES | DYNAMIC ATTRIBUTE ASSOCIATION*

The information system dynamically associates security attributes with [*Assignment: organization-defined subjects and objects*] in accordance with [*Assignment: organization-defined security policies*] as information is created and combined.

Supplemental Guidance: Dynamic association of security attributes is appropriate whenever the security characteristics of information changes over time. Security attributes may change, for example, due to information aggregation issues (i.e., the security characteristics of individual information elements are different from the combined elements), changes in individual access authorizations (i.e., privileges), and changes in the security category of information. Related control: AC-4.

(2) *SECURITY ATTRIBUTES | ATTRIBUTE VALUE CHANGES BY AUTHORIZED INDIVIDUALS*

The information system provides authorized individuals (or processes acting on behalf of individuals) the capability to define or change the value of associated security attributes.

Supplemental Guidance: The content or assigned values of security attributes can directly affect the ability of individuals to access organizational information. Therefore, it is important for information systems to be able to limit the ability to create or modify security attributes to authorized individuals. Related controls: AC-6, AU-2.

(3) *SECURITY ATTRIBUTES | MAINTENANCE OF ATTRIBUTE ASSOCIATIONS BY INFORMATION SYSTEM*

The information system maintains the association and integrity of [*Assignment: organization-defined security attributes*] to [*Assignment: organization-defined subjects and objects*].

Supplemental Guidance: Maintaining the association and integrity of security 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, access control decisions or information flow control decisions.

SECURITY ATTRIBUTES | ASSOCIATION OF ATTRIBUTES BY AUTHORIZED INDIVIDUALS

Deleted: (e.g., records, buffers, files)

Deleted: the

Deleted: system and are used

Deleted: the implementation of access control and flow control policies, reflect special dissemination, handling or distribution instructions, or support other aspects of the information security policy. The term security label is often used to associate a set of security attributes with a specific information object as part of the data structure for that object (

Deleted: .g., user access privileges,

Deleted:).

Deleted: reconfigures

Deleted: an identified

Deleted: policy

Deleted: <#>¶

Deleted: allows authorized entities to

Deleted: .

Deleted: binding

Deleted: information

Deleted: for

Deleted: Examples of automated

Deleted: automated

Deleted: (e.g., Mandatory Access Control

Deleted:), or decisions to release (or not release) information (e.g., information flows via cross domain systems)

The information system supports the association of [*Assignment: organization-defined security attributes*] with [*Assignment: organization-defined subjects and objects*] by authorized individuals (or processes acting on behalf of individuals).

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

Deleted: allows authorized users to associate security attributes with information

Deleted: the

Deleted: system

Deleted: from

Deleted: , to

(4) *SECURITY ATTRIBUTES | ATTRIBUTE DISPLAYS FOR OUTPUT DEVICES*

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

Supplemental Guidance: Information system outputs include, for example, pages, screens, or equivalent. Information system output devices include, for example, printers and video displays on computer workstations, notebook computers, and personal digital assistants.

Deleted: output from the system to system

Deleted: ***set of***

Deleted:

Deleted: Enhancement

Deleted: Objects output from the information

Deleted: Output

Deleted: terminals, monitors, screens on

Deleted: /laptop

(5) *SECURITY ATTRIBUTES | MAINTENANCE OF ATTRIBUTE ASSOCIATION BY ORGANIZATION*

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

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

(6) *SECURITY ATTRIBUTES | CONSISTENT ATTRIBUTE INTERPRETATION*

The organization provides a consistent interpretation of security attributes transmitted between distributed information system components.

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

(7) *SECURITY ATTRIBUTES | ASSOCIATION TECHNIQUES / TECHNOLOGIES*

The information system implements [*Assignment: organization-defined techniques or technologies*] with [*Assignment: organization-defined level of assurance*] in associating security attributes to information.

Supplemental Guidance: The association (i.e., binding) of security attributes to information within information systems is of significant importance with regard to conducting automated access enforcement and flow enforcement actions. The association of such security attributes can be accomplished with technologies/techniques providing different levels of assurance. For example, information systems can cryptographically bind security attributes to information using digital signatures with the supporting cryptographic keys protected by hardware devices (sometimes known as hardware roots of trust).

(8) *SECURITY ATTRIBUTES | ATTRIBUTE REASSIGNMENT*

The organization ensures that security attributes associated with information are reassigned only via re-grading mechanisms validated using [*Assignment: organization-defined techniques or procedures*].

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

(9) *SECURITY ATTRIBUTES | ATTRIBUTE CONFIGURATION BY AUTHORIZED INDIVIDUALS*

The information system provides authorized individuals the capability to define or change the type and value of security attributes available for association with subjects and objects.

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

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

AC-17 REMOTE ACCESS

Control: The organization:

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

b. Authorizes remote access to the information system prior to allowing such connections.

Supplemental Guidance: Remote access is access to organizational information systems by users (or processes acting on behalf of users) communicating through external networks (e.g., the Internet). Remote access methods include, for example, dial-up, broadband, and wireless. Organizations often employ encrypted virtual private networks (VPNs) to enhance confidentiality and integrity over remote connections. The use of encrypted VPNs does not make the access non-remote; however, the use of VPNs, when adequately provisioned with appropriate security controls (e.g., employing appropriate encryption techniques for confidentiality and integrity protection) may provide sufficient assurance to the organization that it can effectively treat such connections as internal networks. Still, VPN connections traverse external networks, and the encrypted VPN does not enhance the availability of remote connections. Also, VPNs with encrypted tunnels can affect the organizational capability to adequately monitor network communications traffic for malicious code. Remote access controls apply to information systems other than public web servers or systems designed for public access. This control addresses authorization prior to allowing remote access without specifying the formats for such authorization. While organizations may use interconnection security agreements to authorize remote access connections, such agreements are not required by this control. Enforcing access restrictions for remote connections is addressed in AC-3. Related controls: AC-2, AC-3, AC-18, AC-19, AC-20, CA-3, CA-7, CM-8, IA-2, IA-3, IA-8, MA-4, PE-17, PL-4, SC-10, SI-4.

Control Enhancements:

(1) *REMOTE ACCESS | AUTOMATED MONITORING / CONTROL*

The information system monitors and controls remote access methods.

Supplemental Guidance: Automated monitoring and control of remote access sessions allows organizations to detect cyber attacks and also ensure ongoing compliance with remote access policies by auditing connection activities of remote users on a variety of information system components (e.g., servers, workstations, notebook computers, smart phones, and tablets). Related controls: AU-2, AU-12.

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

The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

Supplemental Guidance: The encryption strength of mechanism is selected based on the security categorization of the information. Related controls: SC-8, SC-12, SC-13.

(3) *REMOTE ACCESS | MANAGED ACCESS CONTROL POINTS*

Deleted: <#>Documents allowed methods of remote access to the information system;¶

Deleted: allowed

Deleted: method;

Deleted: <#>Monitors for unauthorized remote access to the information system;¶

Deleted: connection; and

Deleted: <#>Enforces requirements for remote connections to the information system.¶

Deleted: This control requires explicit authorization prior to allowing remote access to an information system without specifying a specific format for that authorization. For example, while the organization may deem it appropriate to use a system interconnection ...

Deleted: any

Deleted: an

Deleted: system

Deleted: a user

Deleted: process

Deleted: a user

Deleted: an

Deleted: network

Deleted: Examples of remote

Deleted:

Deleted: (see AC-18 for wireless access). A

Deleted: network

Deleted: , is considered an internal network ...

Deleted: to protect the confidentiality or ...

Deleted: are applicable

Deleted: specifically

Deleted:

Deleted: associated with

Deleted: accomplished by control

Deleted:

Deleted: .

Deleted: Control Enhancements:¶

Deleted: The organization employs ...

Deleted: Enhancement

Deleted: audit user activities

Deleted: /laptop

Deleted:) and to ensure compliance with ...

Deleted: The organization uses ...

Deleted: Enhancement

Deleted: 9

The information system routes all remote accesses through [*Assignment: organization-defined number*] managed network access control points.

Supplemental Guidance: Limiting the number of access control points for remote accesses reduces the attack surface for organizations. Organizations consider the Trusted Internet Connections (TIC) initiative requirements for external network connections. Related control: SC-7.

(4) *REMOTE ACCESS | PRIVILEGED COMMANDS / ACCESS*

The organization:

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

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

Supplemental Guidance: Related control: AC-6.

(5) *REMOTE ACCESS | MONITORING FOR UNAUTHORIZED CONNECTIONS*

[Withdrawn: Incorporated into SI-4].

(6) *REMOTE ACCESS | PROTECTION OF INFORMATION*

The organization ensures that users protect information about remote access mechanisms from unauthorized use and disclosure.

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

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

(8) Related controls: AT-2, AT-3, PS-6. *REMOTE ACCESS | DISABLE NONSECURE NETWORK PROTOCOLS*

[Withdrawn: Incorporated into CM-7].

(9) *REMOTE ACCESS | DISCONNECT / DISABLE ACCESS*

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

Supplemental Guidance: This control enhancement requires organizations to have the capability to rapidly disconnect current users remotely accessing the information system and/or disable further remote access. The speed of disconnect or disablement varies based on the criticality of missions/business functions and the need to eliminate immediate or future remote access to organizational information systems.

References: NIST Special Publications 800-46, 800-77, 800-113, 800-114, 800-121.

Priority and Baseline Allocation:

P1	**LOW** AC-17	**MOD** AC-17 (1) (2) (3) (4)	**HIGH** AC-17 (1) (2) (3) (4)

AC-18 WIRELESS ACCESS

Control: The organization:

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

b. Authorizes wireless access to the information system prior to allowing such connections.

Supplemental Guidance: Wireless technologies include, for example, microwave, packet radio (UHF/VHF), 802.11x, and Bluetooth. Wireless networks use authentication protocols (e.g., EAP/TLS, PEAP), which provide credential protection and mutual authentication. Related controls: AC-2, AC-3, AC-17, AC-19, CA-3, CA-7, CM-8, IA-2, IA-3, IA-8, PL-4, SI-4.

Control Enhancements:

Deleted: a limited

Deleted: of

Deleted: Enhancement

Deleted: authorizes

Deleted: compelling operational

Deleted: documents

Deleted: Enhancement

Deleted: The organization monitors for unauthorized remote connections to the information system [*Assignment: organization-defined frequency*], and takes appropriate action if an unauthorized connection is discovered.¶

Deleted: The organization ensures that remote sessions for accessing [*Assignment: organization-defined list of security functions and security-relevant information*] employ [*Assignment: organization-defined additional security measures*] and are audited.

Deleted: Enhancement Supplemental Guidance: Additional security measures are typically above and beyond standard bulk or session layer encryption (e.g., Secure Shell [SSH], Virtual Private Networking [VPN] with blocking mode enabled).

Deleted: SC-8, SC-9

Deleted: ¶

Deleted: The organization disables [*Assignment: organization-defined networking*

Deleted: *protocols within the information system deemed to be nonsecure*] except for explicitly identified components in support of specific operational requirements.

Deleted: Enhancement Supplemental Guidance: The organization can either make a determination of the relative security of the networking protocol or base the security decision on the assessment of other entities. Bluetooth and peer-to-peer networking are ...

Deleted: (5) (7) (8)

Deleted: (5) (7) (8)

Deleted: <#>Monitors for unauthorized wireless access to the information system;¶

Deleted: connection; and¶
Enforces requirements for wireless

Deleted: to the information system

Deleted: but are not limited to

Deleted: satellite,

Deleted:

Deleted: In certain situations, wireless signals may radiate beyond the confines and control of ...

(1) *WIRELESS ACCESS | AUTHENTICATION AND ENCRYPTION*

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

Supplemental Guidance: Related controls: SC-8, SC-13.

(2) *WIRELESS ACCESS | MONITORING UNAUTHORIZED CONNECTIONS*

[Withdrawn: Incorporated into SI-4].

(3) *WIRELESS ACCESS | DISABLE WIRELESS NETWORKING*

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

Supplemental Guidance: Related control: AC-19.

(4) *WIRELESS ACCESS | RESTRICT CONFIGURATIONS BY USERS*

The organization identifies and explicitly authorizes users allowed to independently configure wireless networking capabilities.

Supplemental Guidance: Organizational authorizations to allow selected users to configure wireless networking capability are enforced in part, by the access enforcement mechanisms employed within organizational information systems. Related controls: AC-3, SC-15.

(5) *WIRELESS ACCESS | ANTENNAS / TRANSMISSION POWER LEVELS*

The organization selects radio antennas and calibrates transmission power levels to reduce the probability that usable signals can be received outside of organization-controlled boundaries.

Supplemental Guidance: Actions that may be taken by organizations to limit unauthorized use of wireless communications outside of organization-controlled boundaries include, for example: (i) reducing the power of wireless transmissions so that the transmissions are less likely to emit a signal that can be used by adversaries outside of the physical perimeters of organizations; (ii) employing measures such as TEMPEST to control wireless emanations; and (iii) using directional/beam forming antennas that reduce the likelihood that unintended receivers will be able to intercept signals. Prior to taking such actions, organizations can conduct periodic wireless surveys to understand the radio frequency profile of organizational information systems as well as other systems that may be operating in the area. Related control: PE-19.

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

Priority and Baseline Allocation:

P1	**LOW** AC-18	**MOD** AC-18 (1)	**HIGH** AC-18 (1) (4) (5)

AC-19 ACCESS CONTROL FOR MOBILE DEVICES

Control: The organization:

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

b. Authorizes the connection of mobile devices to organizational information systems.

Supplemental Guidance: A mobile device is a computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices 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 in close proximity to the individual; however, the degree of proximity can vary depending upon on the form factor and size of the device. The

Deleted: Enhancement

Deleted: Authentication applies to user, device, or both as necessary.

Deleted: control

Deleted: The organization monitors for unauthorized wireless connections to the information system, including scanning for unauthorized wireless access points [*Assignment: organization-defined frequency*], and takes appropriate action if an unauthorized connection is discovered.¶
Enhancement Supplemental Guidance: Organizations proactively search for unauthorized wireless connections including the conduct of thorough scans for unauthorized wireless access points. The scan is not necessarily limited to only those areas within the facility containing the information systems, yet is conducted outside of those areas only as needed to verify that unauthorized wireless access points are not connected to the system.

Deleted: does not allow users

Deleted: confines wireless communications to

Deleted: Enhancement

Deleted: the organization

Deleted: confine

Deleted: to

Deleted: the

Deleted: transmission such

Deleted: it cannot transit

Deleted: perimeter

Deleted: the organization

Deleted: configuring

Deleted: wireless access such that it is point to point in nature

Deleted: 2) (

Deleted: connection of mobile devices meeting organizational usage restrictions and implementation guidance to organizational information systems;¶
<#>Monitors for unauthorized connections of mobile devices to organizational information systems;¶
Enforces requirements for

Deleted: <#>Disables information system functionality that provides the capability for automatic execution of code on mobile devices without user direction;¶
<#>Issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures; and¶
<#>Applies [*Assignment: organization-defined inspection and preventative measures*] to mob ...

processing, storage, and transmission capability of the mobile device may be comparable to or merely a subset of desktop systems, depending upon the nature and intended purpose of the device. Due to the large variety of mobile devices with different technical characteristics and capabilities, organizational restrictions may vary for the different classes/types of such devices. Usage restrictions and specific implementation guidance for mobile devices include, for example, configuration management, device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection, firewall), scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared).

Organizations are cautioned that the need to provide adequate security for mobile devices goes beyond the requirements in this control. Many safeguards and countermeasures for mobile devices are reflected in other security controls in the catalog allocated in the initial control baselines as starting points for the development of security plans and overlays using the tailoring process. There may also be some degree of overlap in the requirements articulated by the security controls within the different families of controls. AC-20 addresses mobile devices that are not organization-controlled. Related controls: AC-3, AC-7, AC-18, AC-20, CA-9, CM-2, IA-2, IA-3, MP-2, MP-4, MP-5, PL-4, SC-7, SC-43, SI-3, SI-4.

Control Enhancements:

(1) *ACCESS CONTROL FOR MOBILE DEVICES | USE OF WRITABLE / PORTABLE STORAGE DEVICES*

[Withdrawn: Incorporated into MP-7].

(2) *ACCESS CONTROL FOR MOBILE DEVICES | USE OF PERSONALLY OWNED PORTABLE STORAGE DEVICES*

[Withdrawn: Incorporated into MP-7].

(3) *ACCESS CONTROL FOR MOBILE DEVICES | USE OF PORTABLE STORAGE DEVICES WITH NO IDENTIFIABLE OWNER*

[Withdrawn: Incorporated into MP-7].

(4) *ACCESS CONTROL FOR MOBILE DEVICES | RESTRICTIONS FOR CLASSIFIED INFORMATION*

The organization:

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

(b) Enforces the following restrictions on individuals permitted by the authorizing official to use unclassified mobile devices in facilities containing information systems processing, storing, or transmitting classified information:

(1) Connection of unclassified mobile devices to classified information systems is prohibited;

(2) Connection of unclassified mobile devices to unclassified information systems requires approval from the authorizing official;

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

(4) Unclassified mobile devices and the information stored on those devices are subject to random reviews and inspections by [*Assignment: organization-defined security officials*], and if classified information is found, the incident handling policy is followed.

(c) Restricts the connection of classified mobile devices to classified information systems in accordance with [*Assignment: organization-defined security policies*].

Supplemental Guidance: Related controls: CA-6, IR-4.

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

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

Supplemental Guidance: Container-based encryption provides a more fine-grained approach to the encryption of data/information on mobile devices, including for example, encrypting

Deleted: Examples of information system functionality that provide the capability for automatic execution of code are AutoRun and AutoPlay.

Deleted: Organizational policies and procedures for mobile devices used by individuals departing on and returning from travel 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 measures to the device after travel is completed. Specially configured mobile devices include, for example, computers with sanitized hard drives, limited applications, and additional hardening (e.g., more stringent configuration settings). Specified measures applied to mobile devices upon return from travel include, for example, examining the device for signs of physical tampering and purging/reimaging the hard disk drive. Protecting information residing on mobile devices is covered in the media protection family. Related controls: MP-4, MP-5.

Deleted: The organization restricts the use of writable, removable media in organizational information systems.¶

Deleted: The organization prohibits the use of personally owned, removable media in organizational information systems.¶

Deleted: The organization prohibits the use of removable media in organizational information systems when the media has

Deleted: no identifiable owner.

Deleted: Enhancement Supplemental Guidance: An identifiable owner (e.g., individual, organization, or project) for removable media helps to reduce the risk of using such technology by assigning responsibility and accountability for addressing known vulnerabilities in the media (e.g.,

Deleted: malicious code insertion).

Deleted: appropriate

Deleted: (s);

Deleted: to use

Deleted: appropriate

Deleted: (s);

Deleted: Mobile

Deleted: /

selected data structures such as files, records, or fields. Related controls: MP-5, SC-13, SC-28.

References: OMB Memorandum 06-16; NIST Special Publications 800-114, 800-124, 800-164.

Priority and Baseline Allocation:

P1	**LOW** AC-19	**MOD** AC-19 (5)	**HIGH** AC-19 (5)

Deleted: (1) (2) (3)

Deleted: (1) (2) (3)

AC-20 USE OF EXTERNAL INFORMATION SYSTEMS

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

a. Access the information system from external information systems; and

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

Deleted: the

Deleted: and/…r transmit organization- ...

Supplemental Guidance: External information systems are information systems or components of information 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 information systems include, for example: (i) personally owned information systems/devices (e.g., notebook computers, smart phones, tablets, personal digital assistants); (ii) privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, train stations, convention centers, shopping malls, or airports); (iii) information systems owned or controlled by nonfederal governmental organizations; and (iv) federal information systems that are not owned by, operated by, or under the direct supervision and authority of organizations. This control also addresses the use of external information systems for the processing, storage, or transmission of organizational information, including, for example, accessing cloud services (e.g., infrastructure as a service, platform as a service, or software as a service) from organizational information systems.

Deleted: the organization…rganizations and ...

For some external information systems (i.e., information systems operated by other federal agencies, including 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. Information systems within these organizations would not be considered external. These situations occur when, for example, there are pre-existing sharing/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, or policies. Authorized individuals include, for example, organizational personnel, contractors, or other individuals with authorized access to organizational information systems and over which organizations have the authority to impose 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 upon the trust relationships between organizations. Therefore, organizations may choose to impose different security restrictions on contractors than on state, local, or tribal governments.

Deleted: , in particular those…(i.e., informat ...

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

Deleted: and information …e.g., individuals ...

restrictions on organizational personnel using those external systems. Related controls: AC-3, AC-17, AC-19, CA-3, PL-4, SA-9.

Control Enhancements:

(1) *USE OF EXTERNAL INFORMATION SYSTEMS | LIMITS ON AUTHORIZED USE*

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

(a) Verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or

Deleted: Can verify

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

Deleted: Has

Supplemental Guidance: This control enhancement recognizes that there are circumstances where individuals using external information systems (e.g., contractors, coalition partners) need to access organizational information systems. In those situations, organizations need confidence that the external information systems contain the necessary security safeguards (i.e., security controls), so as not to compromise, damage, or otherwise harm organizational information systems. Verification that the required security controls have been implemented can be achieved, for example, by third-party, independent assessments, attestations, or other means, depending on the confidence level required by organizations. Related control: CA-2.

(2) *USE OF EXTERNAL INFORMATION SYSTEMS | PORTABLE STORAGE DEVICES*

The organization [*Selection: restricts; prohibits*] the use of organization-controlled portable storage devices by authorized individuals on external information systems.

Deleted: limits

Deleted: media

Supplemental Guidance: Limits on the use of organization-controlled portable storage devices in external information 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.

Deleted: Enhancement

Deleted: media

Deleted: can

(3) *USE OF EXTERNAL INFORMATION SYSTEMS | NON-ORGANIZATIONALLY OWNED SYSTEMS / COMPONENTS / DEVICES*

The organization [*Selection: restricts; prohibits*] the use of non-organizationally owned information systems, system components, or devices to process, store, or transmit organizational information.

Supplemental Guidance: Non-organizationally owned devices include devices owned by other organizations (e.g., federal/state agencies, contractors) and personally owned devices. There are risks to using non-organizationally owned devices. In some cases, the risk is sufficiently high as to prohibit such use. In other cases, it may be such that the use of non-organizationally owned devices is allowed but restricted in some way. Restrictions include, for example: (i) requiring the implementation of organization-approved security controls prior to authorizing such connections; (ii) limiting access to certain types of information, services, or applications; (iii) using virtualization techniques to limit processing and storage activities to servers or other system components provisioned by the organization; and (iv) agreeing to terms and conditions for usage. For personally owned devices, organizations consult with the Office of the General Counsel regarding legal issues associated with using such devices in operational environments, including, for example, requirements for conducting forensic analyses during investigations after an incident.

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

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

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

References: FIPS Publication 199.

Priority and Baseline Allocation:

P1	**LOW** AC-20	**MOD** AC-20 (1) (2)	**HIGH** AC-20 (1) (2)

AC-21 INFORMATION SHARING

Control: The organization:

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

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

Supplemental Guidance: This control applies to information that may be restricted in some manner (e.g., privileged medical information, contract-sensitive information, proprietary information, personally identifiable information, classified information related to special access programs or compartments) based on some formal or administrative determination. Depending on the particular information-sharing circumstances, sharing partners may be defined at the individual, group, or organizational level. Information may be defined by content, type, security category, or special access program/compartment. Related control: AC-3.

Control Enhancements:

(1) *INFORMATION SHARING | AUTOMATED DECISION SUPPORT*

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

(2) *INFORMATION SHARING | INFORMATION SEARCH AND RETRIEVAL*

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

References: None.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** AC-21	**HIGH** AC-21

AC-22 PUBLICLY ACCESSIBLE CONTENT

Control: The organization:

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

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

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

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

Supplemental Guidance: In accordance with federal laws, Executive Orders, directives, policies, regulations, standards, and/or guidance, the general public is not authorized access to nonpublic information (e.g., information protected under the Privacy Act and proprietary information). This control addresses information systems that are controlled by the organization and accessible to the general public, typically without identification or authentication. The posting of information on

Deleted: USER-BASED COLLABORATION AND

Deleted: *list of*

Deleted: *information sharing circumstances and*

Deleted: *required*

Deleted: The

Deleted: /

Deleted:

Deleted: circumstance, the

Deleted: partner

Deleted: organization

Deleted: and information

Deleted: specific

Deleted: or

Deleted: categorization.

Deleted: employs automated mechanisms to enable authorized users to make

Deleted: P0

Deleted: Not Selected

Deleted: Not Selected

Deleted: an organizational information system that is

Deleted: for

Deleted: prior to posting onto the organizational information system;

Deleted: organizational

Deleted:];

Deleted: ¶
Removes nonpublic information from the publicly accessible organizational information system

Deleted: Nonpublic information is any information for which the general public is not authorized access in

Deleted: . Information

Deleted: vendor

Deleted: are examples of nonpublic information.

Deleted: posting

Deleted: on an organizational information system

Deleted: is

Deleted:

non-organization information systems is covered by organizational policy. Related controls: AC-3, AC-4, AT-2, AT-3, AU-13.

Deleted: appropriate

Deleted:

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P3	**LOW** AC-22	**MOD** AC-22	**HIGH** AC-22

Deleted: P2

AC-23 DATA MINING PROTECTION

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

Supplemental Guidance: Data storage objects include, for example, databases, database records, and database fields. Data mining prevention and detection techniques include, for example: (i) limiting the types of responses provided to database queries; (ii) limiting the number/frequency of database queries to increase the work factor needed to determine the contents of such databases; and (iii) 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.

Moved (insertion) [2]

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

AC-24 ACCESS CONTROL DECISIONS

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

Supplemental Guidance: Access control decisions (also known as authorization decisions) occur when authorization information is applied to specific accesses. In contrast, access enforcement occurs when information 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 information systems, different entities may perform access control decisions and access enforcement.

Control Enhancements:

(1) *ACCESS CONTROL DECISIONS | TRANSMIT ACCESS AUTHORIZATION INFORMATION*

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

Supplemental Guidance: In distributed information 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 due to the fact that in distributed information systems, there are various access control decisions that need to be made and different entities (e.g., services) make these decisions in a serial fashion, each requiring some security attributes to make the decisions. Protecting access authorization information (i.e., access control decisions) ensures that such information cannot be altered, spoofed, or otherwise compromised during transmission.

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

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

Supplemental Guidance: In certain situations, it is important that access control decisions can be made without information regarding the identity of the users issuing the requests. These are generally instances where preserving individual privacy is of paramount importance. In other situations, user identification information is simply not needed for access control decisions and, especially in the case of distributed information systems, transmitting such information with the needed degree of assurance may be very expensive or difficult to accomplish.

References: None.

Moved (insertion) [3]

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

AC-25 REFERENCE MONITOR

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

Supplemental Guidance: Information is represented internally within information 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. Reference monitors typically 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 information system strictly enforces the access control policy based on the rule set established by the policy. The *tamperproof* property of the reference monitor prevents adversaries from compromising the functioning of the mechanism. The *always invoked* property prevents adversaries from bypassing the mechanism and hence violating the security policy. The *smallness* property helps to ensure the completeness in the analysis and testing of the mechanism to detect weaknesses or deficiencies (i.e., latent flaws) that would prevent the enforcement of the security policy. Related controls: AC-3, AC-16, SC-3, SC-39.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

FAMILY: AWARENESS AND TRAINING

AT-1 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

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

Deleted: Formal, documented procedures

Deleted: .

b. Reviews and updates the current:

1. Security awareness and training policy [*Assignment: organization-defined frequency*]; and

2. Security awareness and training procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AT family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Deleted: is intended to produce

Deleted: that are required

Deleted: security awareness and training

Deleted: The policy

Deleted: are consistent with

Deleted: policies,

Deleted: Existing organizational

Deleted: additional

Deleted: The security awareness and training

Deleted: organization. Security awareness and training

Deleted: developed

Deleted: a

Deleted: system, when required.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-16, 800-50, 800-100.

Priority and Baseline Allocation:

P1	**LOW** AT-1	**MOD** AT-1	**HIGH** AT-1

AT-2 SECURITY AWARENESS TRAINING

Control: The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors):

a. As part of initial training for new users;

b. When required by information system changes; and

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

Deleted: all

Deleted:) as

Deleted: , when

Deleted: ,

Deleted:

Supplemental Guidance: Organizations determine the appropriate content of security awareness training and security awareness techniques based on the specific organizational requirements and the information systems to which personnel have authorized access. The content includes a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents. The content also addresses awareness of the need for operations security. Security awareness techniques can include, for example, displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from

Deleted: The organization determines

Deleted: of the organization

Moved (insertion) [4]

Deleted:

Moved up [4]: The content includes a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents.

Deleted:

Deleted: as it relates to the organization's information security program.

senior organizational officials, displaying logon screen messages, and conducting information security awareness events. Related controls: AT-3, AT-4, PL-4.

Control Enhancements:

(1) *SECURITY AWARENESS | PRACTICAL EXERCISES*

The organization includes practical exercises in security awareness training that simulate actual cyber attacks.

Supplemental Guidance: Practical exercises may include, for example, no-notice social engineering attempts to collect information, gain unauthorized access, or simulate the adverse impact of opening malicious email attachments or invoking, via spear phishing attacks, malicious web links. Related controls: CA-2, CA-7, CP-4, IR-3.

Deleted: Enhancement

(2) *SECURITY AWARENESS | INSIDER THREAT*

The organization includes security awareness training on recognizing and reporting potential indicators of insider threat.

Supplemental Guidance: Potential indicators and possible precursors of insider threat can include behaviors such as inordinate, long-term job dissatisfaction, attempts to gain access to information not required for job performance, unexplained access to financial resources, bullying or sexual harassment of fellow employees, workplace violence, and other serious violations of organizational policies, procedures, directives, rules, or practices. Security awareness training includes how to communicate employee and management concerns regarding potential indicators of insider threat through appropriate organizational channels in accordance with established organizational policies and procedures. Related controls: PL-4, PM-12, PS-3, PS-6.

References: C.F.R. Part 5 Subpart C (5 C.F.R 930.301); Executive Order 13587; NIST Special Publication 800-50.

Priority and Baseline Allocation:

P1	**LOW** AT-2	**MOD** AT-2 (2)	**HIGH** AT-2 (2)

AT-3 ROLE-BASED SECURITY TRAINING

Control: The organization provides role-based security training to personnel with assigned security roles and responsibilities:

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

b. When required by information system changes; and

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

Deleted: -related

Deleted: : (i) before

Deleted: (ii) when

Deleted: (iii)

Supplemental Guidance: Organizations determine the appropriate content of security training based on the assigned roles and responsibilities of individuals and the specific security requirements of organizations and the information systems to which personnel have authorized access. In addition, organizations provide enterprise architects, information system developers, software developers, acquisition/procurement officials, information system managers, system/network administrators, personnel conducting configuration management and auditing activities, personnel performing independent verification and validation activities, security control assessors, and other personnel having access to system-level software, adequate security-related technical training specifically tailored for their assigned duties. 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, and artifacts for the organizational security roles defined. Organizations also provide the training necessary for individuals to carry out their responsibilities related to operations and supply chain security within the context of organizational information security programs. Role-

Deleted: The organization determines

Deleted: the organization

Deleted:

Deleted: the organization provides

Deleted: and

Deleted: to perform

Deleted: Organizational security

Deleted: The organization

Deleted: provides

Deleted: these

Deleted: the organization's

Deleted: program.

based security training also applies to contractors providing services to federal agencies. Related controls: AT-2, AT-4, PL-4, PS-7, SA-3, SA-12, SA-16.

Control Enhancements:

(1) *SECURITY TRAINING | ENVIRONMENTAL CONTROLS*

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

Deleted: employees

Supplemental Guidance: Environmental controls include, for example, fire suppression and detection devices/systems, sprinkler systems, handheld fire extinguishers, fixed fire hoses, smoke detectors, temperature/humidity, HVAC, and power within the facility. Organizations identify personnel with specific roles and responsibilities associated with environmental controls requiring specialized training. Related controls: PE-1, PE-13, PE-14, PE-15.

Deleted: Enhancement

(2) *SECURITY TRAINING | PHYSICAL SECURITY CONTROLS*

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

Deleted: employees

Supplemental Guidance: Physical security controls include, for example, physical access control devices, physical intrusion alarms, monitoring/surveillance equipment, and security guards (deployment and operating procedures). Organizations identify personnel with specific roles and responsibilities associated with physical security controls requiring specialized training. Related controls: PE-2, PE-3, PE-4, PE-5.

Deleted: Enhancement

Deleted: and

(3) *SECURITY TRAINING | PRACTICAL EXERCISES*

The organization includes practical exercises in security training that reinforce training objectives.

Supplemental Guidance: Practical exercises may include, for example, security training for software developers that includes simulated cyber attacks exploiting common software vulnerabilities (e.g., buffer overflows), or spear/whale phishing attacks targeted at senior leaders/executives. These types of practical exercises help developers better understand the effects of such vulnerabilities and appreciate the need for security coding standards and processes.

(4) *SECURITY TRAINING | SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR*

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

Supplemental Guidance: A well-trained workforce provides another organizational safeguard that can be employed as part of a defense-in-depth strategy to protect organizations against malicious code coming in to organizations via email or the web applications. Personnel are trained to look for indications of potentially suspicious email (e.g., 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 such suspicious email or web communications (e.g., not opening attachments, not clicking on embedded web links, and checking the source of email addresses). For this process to work effectively, all organizational personnel are trained and made aware of what constitutes suspicious communications. Training personnel on how to recognize anomalous behaviors in organizational information 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.

References: C.F.R. Part 5 Subpart C (5 C.F.R. 930.301); NIST Special Publications 800-16, 800-50.

Priority and Baseline Allocation:

P1	**LOW** AT-3	**MOD** AT-3	**HIGH** AT-3

AT-4 SECURITY TRAINING RECORDS

Control: The organization:

a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and

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

Supplemental Guidance: Documentation for specialized training may be maintained by individual supervisors at the option of the organization. Related controls: AT-2, AT-3, PM-14.

Deleted: Supplemental Guidance: While an organization may deem that organizationally mandated individual training programs and the development of individual training plans are necessary, this control does not mandate either.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P3	**LOW** AT-4	**MOD** AT-4	**HIGH** AT-4

AT-5 CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS

[Withdrawn: Incorporated into PM-15].

Deleted: Control: The organization establishes and institutionalizes contact with selected groups and associations within the security community:¶

<#>To facilitate ongoing security education and training for organizational personnel;¶

<#>To stay up to date with the latest recommended security practices, techniques, and technologies; and¶

<#>To share current security-related information including threats, vulnerabilities, and incidents.¶

Supplemental Guidance: Ongoing contact with security groups and associations is of paramount importance in an environment of rapid technology changes and dynamic threats. Security groups and associations can include, for example, special interest groups, specialized forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations. The groups and associations selected are consistent with the organization's mission/business requirements. Information-sharing activities regarding threats, vulnerabilities, and incidents related to information systems are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance

Moved up [2]: .¶
Control Enhancements: None.¶

Moved up [3]: References: None.¶
Priority and Baseline Allocation:¶
P0

FAMILY: AUDIT AND ACCOUNTABILITY

AU-1 AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

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

b. Reviews and updates the current:

1. Audit and accountability policy [*Assignment: organization-defined frequency*]; and

2. Audit and accountability procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AU family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

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

Priority and Baseline Allocation:

P1	**LOW** AU-1	**MOD** AU-1	**HIGH** AU-1

AU-2 AUDIT EVENTS

Control: The organization:

a. Determines that the information system is capable of auditing the following events: [*Assignment: organization-defined auditable events*];

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

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

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

Supplemental Guidance: An event is any observable occurrence in an organizational information system. Organizations identify audit events as those events which are significant and relevant to

Deleted:
CLASS: TECHNICAL

Deleted: develops,

Deleted: , and reviews/updates

Deleted: *frequency*

Deleted: A formal, documented

Deleted: Formal, documented procedures

Deleted: .

Deleted: is intended to produce

Deleted: that are required

Deleted: audit and accountability

Deleted: The policy

Deleted: are consistent with

Deleted: policies,

Deleted: Existing organizational

Deleted: additional

Deleted:

Deleted: audit and accountability

Deleted: the organization. Audit and accountability procedures

Deleted: developed

Deleted: a

Deleted: system, when required.

Deleted: the development of the audit and accountability

Deleted: .

Deleted: AUDITABLE

Deleted: , based on a risk assessment and mission/business needs,

Deleted: must be

Deleted: *list of*

Deleted: list of

Deleted: , based on current threat information and ongoing assessment of risk,

Deleted: . *to be audited*

Deleted: The purpose of this control

Deleted: for the organization to

Deleted: need to be auditable as

the security of information systems and the environments in which those systems operate in order to meet specific and ongoing audit needs. Audit events can include, for example, password changes, failed logons, or failed accesses related to information systems, administrative privilege usage, PIV credential usage, or third-party credential usage. In determining the set of auditable events, organizations consider the auditing appropriate for each of the security controls to be implemented. To balance auditing requirements with other information system needs, this control also requires identifying that subset of *auditable* events that are *audited* at a given point in time. For example, organizations may determine that information 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 controls and control enhancements. Organizations also include auditable events that are required by applicable federal laws, Executive Orders, directives, policies, regulations, and standards. Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the appropriate level of abstraction is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. Organizations consider in the definition of auditable events, the auditing necessary to cover related events such as the steps in distributed, transaction-based processes (e.g., processes that are distributed across multiple organizations) and actions that occur in service-oriented architectures. Related controls: AC-6, AC-17, AU-3, AU-12, MA-4, MP-2, MP-4, SI-4.

Deleted: the

Deleted: system; giving an overall system requirement

Deleted: ongoing and specific audit needs.

Deleted: to be

Deleted:

Deleted: the organization

Deleted: the

Deleted: system

Deleted: extreme burden on system performance. In addition, audit

Deleted:

Deleted: right

Deleted: for audit record generation

Deleted: Related control: AU-3

Control Enhancements:

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

[Withdrawn: Incorporated into AU-12].

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

[Withdrawn: Incorporated into AU-12].

(3) *AUDIT EVENTS | REVIEWS AND UPDATES*

The organization reviews and updates the audited events [*Assignment: organization-defined frequency*].

Deleted: list of auditable

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

Deleted: Enhancement Supplemental Guidance: The list of auditable events is defined in AU-2.¶

(4) *AUDIT EVENTS | PRIVILEGED FUNCTIONS*

[Withdrawn: Incorporated into AC-6].

Deleted: The organization includes execution of

Deleted: privileged functions in the list of events to be audited by the information system.

References: NIST Special Publication 800-92; Web: csrc.nist.gov/pcig/cig.html, idmanagement.gov.

Priority and Baseline Allocation:

P1	**LOW** AU-2	**MOD** AU-2 (3)	**HIGH** AU-2 (3)

Deleted: (4)

Deleted: (4)

AU-3 CONTENT OF AUDIT RECORDS

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

Supplemental Guidance: Audit record content that may be necessary to satisfy the requirement of this control, includes, for example, time stamps, source and destination addresses, user/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

Deleted: produces

Deleted: that contain sufficient

Deleted: to, at a minimum, establish

Deleted: (date and time)

Deleted: (success or failure)

Deleted: user/subject

Deleted: Related controls: AU-2, AU-8 event-specific results (e.g., the security state of the information system after the event occurred). Related controls: AU-2, AU-8, AU-12, SI-11.

Control Enhancements:

(1) *CONTENT OF AUDIT RECORDS | ADDITIONAL AUDIT INFORMATION*

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

Supplemental Guidance: 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.

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

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

Supplemental Guidance: This control enhancement requires that the content to be captured in audit records be configured from a central location (necessitating automation). Organizations coordinate the selection of required audit content to support the centralized management and configuration capability provided by the information system. Related controls: AU-6, AU-7.

References: None.

Priority and Baseline Allocation:

P1	**LOW** AU-3	**MOD** AU-3 (1)	**HIGH** AU-3 (1) (2)

AU-4 AUDIT STORAGE CAPACITY

Control: The organization allocates audit record storage capacity in accordance with [*Assignment: organization-defined audit record storage requirements*].

Supplemental Guidance: Organizations consider the types of auditing to be performed and the audit processing requirements when allocating audit storage capacity. Allocating sufficient audit storage capacity reduces the likelihood of such capacity being exceeded and resulting in the potential loss or reduction of auditing capability. Related controls: AU-2, AU-5, AU-6, AU-7, AU-11, SI-4.

Control Enhancements:

(1) *AUDIT STORAGE CAPACITY | TRANSFER TO ALTERNATE STORAGE*

The information system off-loads audit records [*Assignment: organization-defined frequency*] onto a different system or media than the system being audited.

Supplemental Guidance: Off-loading is a process designed to preserve the confidentiality and integrity of audit records by moving the records from the primary information system to a secondary or alternate system. It is a common process in information 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.

References: None.

Priority and Baseline Allocation:

Deleted: includes

Deleted:] in the audit records for audit events identified by type, location, or subject.

Deleted: Enhancement

Deleted: An

Deleted: of detailed information that the organization may require in audit records is

Deleted: -

Deleted: The organization centrally manages the

Deleted: and configures auditing to reduce the likelihood of such capacity being exceeded.

Deleted: The organization considers

Deleted: None

P1	**LOW** AU-4	**MOD** AU-4	**HIGH** AU-4

AU-5 RESPONSE TO AUDIT PROCESSING FAILURES

Control: The information system:

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

Deleted: Alerts designated organizational officials

b. Takes the following additional actions: [*Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)*].

Deleted:

Supplemental Guidance: Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded. Organizations may choose to define additional actions for different audit processing failures (e.g., by type, by location, by severity, or a combination of such factors). This control applies to each audit data storage repository (i.e., distinct information system component where audit records are stored), the total audit storage capacity of organizations (i.e., all audit data storage repositories combined), or both. Related controls: AU-4, SI-12.

Deleted: Related control: AU-4

Control Enhancements:

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

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

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

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

The information system provides an alert in [*Assignment: organization-defined real-time period*] to [*Assignment: organization-defined personnel, roles, and/or locations*] when the following audit failure events occur: [*Assignment: organization-defined audit failure events requiring real-time alerts*].

Deleted: a real-time

Supplemental Guidance: Alerts provide organizations with urgent messages. Real-time alerts provide these messages at information technology speed (i.e., the time from event detection to alert occurs in seconds or less).

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

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

Deleted: representing

Deleted: for network traffic

Deleted: *or*

Supplemental Guidance: Organizations have the capability to reject or delay the processing of network communications traffic if auditing such traffic is determined to exceed the storage capacity of the information 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.

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

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

Deleted: an

Deleted: failure,

Deleted: alternative

Supplemental Guidance: Organizations determine the types of audit failures that can trigger automatic information system shutdowns or degraded operations. Because of the importance of ensuring mission/business continuity, organizations may determine that the nature of the audit failure is not so severe that it warrants a complete shutdown of the information system supporting the core organizational missions/business operations. In those instances, partial information system shutdowns or operating in a degraded mode with reduced capability may be viable alternatives. Related control: AU-15.

References: None.

Priority and Baseline Allocation:

P1	**LOW** AU-5	**MOD** AU-5	**HIGH** AU-5 (1) (2)

AU-6 AUDIT REVIEW, ANALYSIS, AND REPORTING

Control: The organization:

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

Deleted: , and reports findings to designated organizational officials;

b. Reports findings to [*Assignment: organization-defined personnel or roles*].

Deleted: <#>Adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to organizational operations, organizational assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.¶
Supplemental Guidance: Related control: AU-7. ¶
¶

Supplemental Guidance: Audit review, analysis, and reporting covers information security-related auditing performed by organizations including, for example, auditing that results from monitoring of account usage, remote access, wireless connectivity, mobile device connection, configuration settings, system component inventory, use of maintenance tools and nonlocal maintenance, physical access, temperature and humidity, equipment delivery and removal, communications at the information system boundaries, use of mobile code, and use of VoIP. Findings can be reported to organizational entities that include, for example, incident response team, help desk, information security group/department. If organizations are prohibited from reviewing and analyzing audit information or unable to conduct such activities (e.g., in certain national security applications or systems), the review/analysis may be carried out by other organizations granted such authority. Related controls: AC-2, AC-3, AC-6, AC-17, AT-3, AU-7, AU-16, CA-7, CM-5, CM-10, CM-11, IA-3, IA-5, IR-5, IR-6, MA-4, MP-4, PE-3, PE-6, PE-14, PE-16, RA-5, SC-7, SC-18, SC-19, SI-3, SI-4, SI-7.

Control Enhancements:

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

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

Deleted: The information system integrates

Supplemental Guidance: Organizational processes benefiting from integrated audit review, analysis, and reporting include, for example, incident response, continuous monitoring, contingency planning, and Inspector General audits. Related controls: AU-12, PM-7.

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

[Withdrawn: Incorporated into SI-4].

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

The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.

Supplemental Guidance: Organization-wide situational awareness includes awareness across all three tiers of risk management (i.e., organizational, mission/business process, and information system) and supports cross-organization awareness. Related controls: AU-12, IR-4.

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

The information system provides the capability to centrally review and analyze audit records from multiple components within the system.

Deleted: centralizes

Deleted: analysis of

Supplemental Guidance: Automated mechanisms for centralized reviews and analyses include, for example, Security Information Management products. Related controls: AU-2, AU-12.

Deleted: Enhancement

Deleted: An example of an automated mechanism

Deleted: review and analysis is a

Deleted: (SIM) product.

Deleted: control

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

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

Supplemental Guidance: This control enhancement does not require vulnerability scanning, the generation of performance data, or information 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 information system components as well as audit record correlation and analysis. The use of standardized audit record analysis scripts developed by organizations (with localized script adjustments, as necessary) provides more cost-effective approaches for analyzing audit record information collected. The correlation of audit record information with vulnerability scanning information is important in determining the veracity of vulnerability scans and correlating attack detection events with scanning results. Correlation with performance data can help uncover denial of service attacks or cyber attacks resulting in unauthorized use of resources. Correlation with system monitoring information can assist in uncovering attacks and in better relating audit information to operational situations. Related controls: AU-12, IR-4, RA-5.

(6) *AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATION WITH PHYSICAL MONITORING*

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

Supplemental Guidance: The correlation of physical audit information and audit logs from information systems may assist organizations in identifying examples of suspicious behavior or supporting evidence of such behavior. For example, the correlation of an individual's identify for logical access to certain information systems with the additional physical security information that the individual was actually present at the facility when the logical access occurred, may prove to be useful in investigations.

(7) *AUDIT REVIEW, ANALYSIS, AND REPORTING | PERMITTED ACTIONS*

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

Supplemental Guidance: Organizations specify permitted actions for information 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 information system and include, for example, read, write, execute, append, and delete.

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

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

Supplemental Guidance: This control enhancement requires a distinct environment for the dedicated analysis of audit information related to privileged users without compromising such information on the information system where the users have elevated privileges including the capability to execute privileged commands. Full text analysis refers to analysis that considers the full text of privileged commands (i.e., commands and all parameters) as opposed to analysis that considers only the name of the command. Full text analysis includes, for example, the use of pattern matching and heuristics. Related controls: AU-3, AU-9, AU-11, AU-12.

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

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

Supplemental Guidance: Nontechnical sources include, for example, human resources records documenting organizational policy violations (e.g., sexual harassment incidents, improper use of organizational information assets). Such information can lead organizations to a more

Deleted: ,

Deleted: , and network

Deleted: Enhancement Supplemental Guidance: A

Deleted: /

Deleted: system tool

Deleted: and

Deleted:

Deleted: the organization

Deleted:),

Deleted: a

Deleted: approach

Deleted:

Deleted: the

Deleted: control

Deleted: 7

Deleted: , SI-4

Deleted: Enhancement Supplemental Guidance: Related control: PE-6.¶

Deleted: authorized

Deleted: ,

Deleted: , and/or

Deleted: in

Deleted: and accountability policy

Deleted: Enhancement

Deleted: Permitted

Deleted: -

directed analytical effort to detect potential malicious insider activity. Due to the sensitive nature of the information available from nontechnical sources, organizations limit access to such information to minimize the potential for the inadvertent release of privacy-related information to individuals that do not have a need to know. Thus, correlation of information from nontechnical sources with audit information generally occurs only when individuals are suspected of being involved in a security incident. Organizations obtain legal advice prior to initiating such actions. Related control: AT-2.

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

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

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

References: None.

Priority and Baseline Allocation:

P1	**LOW** AU-6	**MOD** AU-6 (1) (3)	**HIGH** AU-6 (1) (3) (5) (6)

AU-7 AUDIT REDUCTION AND REPORT GENERATION

Control: The information system provides an audit reduction and report generation capability that:

Deleted: .

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

Deleted: .

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

Deleted:

Supplemental Guidance: Audit reduction is a process that manipulates collected audit information and organizes such information in a summary format that is more meaningful to analysts. Audit reduction and report generation capabilities do not always emanate from the same information 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 information system can generate customizable reports. Time ordering of audit records can be a significant issue if the granularity of the timestamp in the record is insufficient. Related control: AU-6.

Deleted: An audit reduction and report generation capability provides support for near real-time

Deleted: audit review, analysis, and reporting requirements described in AU-6 and after-the-fact investigations of security incidents. Audit reduction and reporting tools do not alter original audit records.

Control Enhancements:

(1) *AUDIT REDUCTION AND REPORT GENERATION | AUTOMATIC PROCESSING*

The information system provides the capability to process audit records for events of interest based on [*Assignment: organization-defined audit fields within audit records*].

Deleted: automatically

Deleted: selectable

Supplemental Guidance: Events of interest can be identified by the content of specific audit record fields including, for example, identities of individuals, event types, event locations, event times, event dates, system resources involved, IP 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 (e.g., by network or subnetwork) or selectable by specific information system component. Related controls: AU-2, AU-12.

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

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

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

References: None.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** AU-7 (1)	**HIGH** AU-7 (1)

AU-8 TIME STAMPS

Control: The information system:

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

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

Deleted: uses

Deleted: .

Supplemental Guidance: Time stamps generated by the information 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 information system clocks and reference clocks, for example, clocks synchronizing within hundreds of milliseconds or within tens of milliseconds. Organizations may define different time granularities for different system components. Time service can also be critical to other security capabilities such as access control and identification and authentication, depending on the nature of the mechanisms used to support those capabilities. Related controls: AU-3, AU-12.

Deleted: both

Deleted: The time may be

Deleted: Related control: AU-3

Control Enhancements:

(1) *TIME STAMPS | SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE*

The information system:

(a) Compares the internal information system clocks [*Assignment: organization-defined frequency*] with [*Assignment: organization-defined authoritative time source*]; and

(b) Synchronizes the internal system clocks to the authoritative time source when the time difference is greater than [*Assignment: organization-defined time period*].

Deleted: synchronizes

Deleted:].

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

(2) *TIME STAMPS | SECONDARY AUTHORITATIVE TIME SOURCE*

The information system identifies a secondary authoritative time source that is located in a different geographic region than the primary authoritative time source.

References: None.

Priority and Baseline Allocation:

P1	**LOW** AU-8	**MOD** AU-8 (1)	**HIGH** AU-8 (1)

AU-9 PROTECTION OF AUDIT INFORMATION

Control: The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

Supplemental Guidance: Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity. This control focuses on technical protection of audit information. Physical protection of audit information is addressed by media protection controls and physical and environmental protection controls. Related controls: AC-3, AC-6, MP-2, MP-4, PE-2, PE-3, PE-6.

Deleted: Related controls: AC-3, AC

Control Enhancements:

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

The information system writes audit trails to hardware-enforced, write-once media.

Supplemental Guidance: This control enhancement applies to the initial generation of audit trails (i.e., the collection of audit records that represents the audit information to be used for detection, analysis, and reporting purposes) and to the backup of those audit trails. The enhancement does not apply to the initial generation of audit records prior to being written to an audit trail. Write-once, read-many (WORM) media includes, for example, Compact Disk-Recordable (CD-R) and Digital Video Disk-Recordable (DVD-R). In contrast, the use of switchable write-protection media such as on tape cartridges or Universal Serial Bus (USB) drives results in write-protected, but not write-once, media. Related controls: AU-4, AU-5.

(2) *PROTECTION OF AUDIT INFORMATION | AUDIT BACKUP ON SEPARATE PHYSICAL SYSTEMS / COMPONENTS*

The information system backs up audit records [*Assignment: organization-defined frequency*] onto a physically different system or system component than the system or component being audited.

Supplemental Guidance: This control enhancement helps to ensure that a compromise of the information system being audited does not also result in a compromise of the audit records. Related controls: AU-4, AU-5, AU-11.

(3) *PROTECTION OF AUDIT INFORMATION | CRYPTOGRAPHIC PROTECTION*

The information system implements cryptographic mechanisms to protect the integrity of audit information and audit tools.

Supplemental Guidance: Cryptographic mechanisms used for protecting the integrity of audit information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the secret key used to generate the hash. Related controls: AU-10, SC-12, SC-13.

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

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

Supplemental Guidance: Individuals with privileged access to an information system and who are also the subject of an audit by that system, may affect the reliability of audit information by inhibiting audit activities or modifying audit records. This control enhancement requires that privileged access be further defined between audit-related privileges and other privileges, thus limiting the users with audit-related privileges. Related control: AC-5.

(5) *PROTECTION OF AUDIT INFORMATION | DUAL AUTHORIZATION*

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

Supplemental Guidance: Organizations may choose different selection options for different types of audit information. Dual authorization mechanisms require the approval of two authorized individuals in order to execute. Related controls: AC-3, MP-2.

(6) *PROTECTION OF AUDIT INFORMATION | READ ONLY ACCESS*

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

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

References: None.

Priority and Baseline Allocation:

P1	**LOW** AU-9	**MOD** AU-9 (4)	**HIGH** AU-9 (2) (3) (4)

Deleted: produces

Deleted: records on

Deleted: media

Deleted: uses

Deleted: Enhancement

Deleted: An example of a cryptographic mechanism

Deleted: protection of

Deleted: is the computation and application of a cryptographic-

Deleted: , protecting the

Deleted: , and using the public key to verify the hash information

Deleted: :¶
Authorizes

Deleted: a limited

**Deleted: privileged users; and¶
Protects the audit records of non-local accesses to *privileged* accounts**

Deleted: and the execution of privileged functions.

Deleted: <#>¶
Enhancement

Deleted: Auditing

Deleted: not be reliable when performed by

Deleted: system to which the user being audited has privileged access. The privileged user may inhibit auditing

Deleted: modify

Deleted:

Deleted: helps mitigate this risk by requiring

Deleted: ,

Deleted: Reducing the risk of audit compromises by privileged users can also be achieved, for example, by performing audit activity on a separate information system or by using storage media that cannot be modified (e.g., write-once recording devices).

AU-10 NON-REPUDIATION

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

Supplemental Guidance: Types of individual actions covered by non-repudiation include, for example, creating information, sending and receiving messages, approving information (e.g., indicating concurrence or signing a contract). Non-repudiation protects individuals against later claims by: (i) authors of not having authored particular documents; (ii) senders of not having transmitted messages; (iii) receivers of not having received messages; or (iv) signatories of not having signed documents. Non-repudiation services can be used to determine if information originated from a particular individual, or if an individual took specific actions (e.g., sending an email, signing a contract, approving a procurement request) or received specific information. Organizations obtain non-repudiation services by employing various techniques or mechanisms (e.g., digital signatures, digital message receipts). Related controls: SC-12, SC-8, SC-13, SC-16, SC-17, SC-23.

Control Enhancements:

(1) *NON-REPUDIATION | ASSOCIATION OF IDENTITIES*

The information system:

(a) Binds the identity of the information producer with the information to [*Assignment: organization-defined strength of binding*]; and

(b) Provides the means for authorized individuals to determine the identity of the producer of the information.

Supplemental Guidance: This control enhancement supports audit requirements that provide organizational personnel with the means to identify who produced specific information in the event of an information transfer. Organizations determine and approve the strength of the binding between the information producer and the information based on the security category of the information and relevant risk factors. Related controls: AC-4, AC-16.

(2) *NON-REPUDIATION | VALIDATE BINDING OF INFORMATION PRODUCER IDENTITY*

The information system:

(a) Validates the binding of the information producer identity to the information at [*Assignment: organization-defined frequency*]; and

(b) Performs [*Assignment: organization-defined actions*] in the event of a validation error.

Supplemental Guidance: This control enhancement prevents the modification of information between production and review. The validation of bindings can be achieved, for example, by the use of cryptographic checksums. Organizations determine if validations are in response to user requests or generated automatically. Related controls: AC-3, AC-4, AC-16.

(3) *NON-REPUDIATION | CHAIN OF CUSTODY*

The information system maintains reviewer/releaser identity and credentials within the established chain of custody for all information reviewed or released.

Supplemental Guidance: Chain of custody is a process that tracks the movement of evidence through its collection, safeguarding, and analysis life cycle by documenting each person who handled the evidence, the date and time it was collected or transferred, and the purpose for the transfer. If the reviewer is a human or if the review function is automated but separate from the release/transfer function, the information system associates the identity of the reviewer of the information to be released with the information and the information label. In the case of human reviews, this control enhancement provides organizational officials the means to identify who reviewed and released the information. In the case of automated reviews, this control enhancement ensures that only approved review functions are employed. Related controls: AC-4, AC-16.

(4) *NON-REPUDIATION | VALIDATE BINDING OF INFORMATION REVIEWER IDENTITY*

The information system:

Deleted: a particular action.

Deleted: Examples of particular

Deleted: actions taken

Deleted: individuals

Deleted: a message

Deleted:), and receiving a message.

Deleted: an author

Deleted: a

Deleted: document, a sender

Deleted: a message, a receiver

Deleted: a message,

Deleted: a signatory

Deleted: a document.

Deleted: an

Deleted: Non

Deleted: are obtained

Deleted: associates

Deleted: .

Deleted: Enhancement

Deleted: appropriate

Deleted: officials

Deleted: The nature and

Deleted: are determined and approved by the appropriate organizational officials

Deleted: categorization

Deleted: validates the binding of the information producer's identity to the information.

Deleted: Enhancement

Deleted: is intended to mitigate

Deleted: risk that

Deleted: is modified

Deleted:

Deleted: Enhancement

Deleted:

Deleted: appropriate

Deleted:

Deleted: helps ensure

Deleted: validates

(a) **Validates the binding of the information reviewer identity to the information at the transfer or release points prior to release/transfer between [*Assignment: organization-defined* security *domains*]; and**

(b) **Performs [*Assignment: organization-defined actions*] in the event of a validation error.**

Supplemental Guidance: This control enhancement prevents the modification of information between review and transfer/release. The validation of bindings can be achieved, for example, by the use of cryptographic checksums. Organizations determine validations are in response to user requests or generated automatically. Related controls: AC-4, AC-16.

(5) *NON-REPUDIATION | DIGITAL SIGNATURES*

[Withdrawn: Incorporated into SI-7].

References: None.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** Not Selected	**HIGH** AU-10

Deleted: reviewer's

Deleted: /

Deleted: point

Deleted: from one

Deleted: domain to another security domain.

Deleted: Enhancement

Deleted: is intended to mitigate

Deleted: risk that

Deleted: is modified

Deleted: ¶

Deleted: organization employs [*Selection: FIPS-validated; NSA-approved*] cryptography to implement digital signatures.

Deleted: Enhancement Supplemental Guidance: Related control: SC-13.¶

Deleted: P1

AU-11 AUDIT RECORD RETENTION

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

Supplemental Guidance: Organizations retain audit records until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoenas, and law enforcement actions. Organizations develop standard categories of audit records relative to such types of actions and standard response processes for each type of action. The National Archives and Records Administration (NARA) General Records Schedules provide federal policy on record retention. Related controls: AU-4, AU-5, AU-9, MP-6.

(1) Control Enhancements: *AUDIT RECORD RETENTION | LONG-TERM RETRIEVAL CAPABILITY*

The organization employs [*Assignment: organization-defined measures*] to ensure that long-term audit records generated by the information system can be retrieved.

Supplemental Guidance: 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.

References: None.

Priority and Baseline Allocation:

P3	**LOW** AU-11	**MOD** AU-11	**HIGH** AU-11

Deleted: The organization retains

Deleted:

Deleted: subpoena

Deleted: Standard categorizations

Deleted: are developed and disseminated.

Deleted: (GRS)

Deleted: None.¶

AU-12 AUDIT GENERATION

Control: The information system:

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

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

c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.

Deleted: list of

Deleted: designated organizational

Deleted: list of audited

Deleted: as

Supplemental Guidance: Audit records can be generated from many different information system components. The list of audited events is the set of events for which audits are to be generated. These events are typically a subset of all events for which the information system is capable of generating audit records. Related controls: AC-3, AU-2, AU-3, AU-6, AU-7.

Control Enhancements:

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

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

Supplemental Guidance: Audit trails are time-correlated if the time stamps in the individual audit records can be reliably related to the time stamps in other audit records to achieve a time ordering of the records within organizational tolerances. Related controls: AU-8, AU-12.

(2) *AUDIT GENERATION | STANDARDIZED FORMATS*

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

Supplemental Guidance: Audit information that is normalized to common standards promotes interoperability and exchange of such information between dissimilar devices and information 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 information systems do not conform to standardized formats, systems may convert individual audit records into standardized formats when compiling system-wide audit trails.

(3) *AUDIT GENERATION | CHANGES BY AUTHORIZED INDIVIDUALS*

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

Supplemental Guidance: This control enhancement enables organizations to extend or limit auditing as necessary to meet organizational requirements. Auditing that is limited to conserve information system resources may be extended to address certain threat situations. In addition, auditing may be limited to a specific set of events to facilitate audit reduction, analysis, and reporting. Organizations can establish time thresholds in which audit actions are changed, for example, near real-time, within minutes, or within hours. Related control: AU-7.

P1	**LOW** AU-12	**MOD** AU-12	**HIGH** AU-12 (1) (3)

AU-13 MONITORING FOR INFORMATION DISCLOSURE

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

Supplemental Guidance: Open source information includes, for example, social networking sites. Related controls: PE-3, SC-7.

Control Enhancements:

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

The organization employs automated mechanisms to determine if organizational information has been disclosed in an unauthorized manner.

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

Deleted: Audits

Deleted: various components within the

Deleted: .

Deleted: This set of

Deleted: is

Deleted: the list of

Deleted: (i.e., auditable events).

Deleted: Enhancement

Deleted: The audit trail is

Deleted: stamp

Deleted: stamp

Deleted: the organization-defined tolerance

Deleted: Enhancement

Deleted: a

Deleted: standard

Deleted:

Deleted: an audit system that produces

Deleted: System

Deleted: the

Deleted: Expression

Deleted:) are examples of standard formats for audit records.

Deleted: individual

Deleted: the

Deleted: system

Deleted: a

Deleted: format, the system

Deleted: a

Deleted: format

Deleted: the

Deleted: trail

Deleted: exfiltration or

Deleted: [*Assignment: organization-defined frequency*].

Deleted: None.

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

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

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

AU-14 SESSION AUDIT

Control: The information system provides the capability for authorized users to select a user session to capture/record or view/hear.

Supplemental Guidance: Session audits include, for example, monitoring keystrokes, tracking websites visited, and recording information and/or file transfers. Session auditing activities are developed, integrated, and used in consultation with legal counsel in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, or standards. Related controls: AC-3, AU-4, AU-5, AU-9, AU-11.

Deleted: to:¶
Capture/record and log all content related to

Deleted: ; and¶
Remotely

Deleted: all content related to an established user session in real time

Deleted: or

Control Enhancements:

(1) *SESSION AUDIT | SYSTEM START-UP*

The information system initiates session audits at system start-up.

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

The information system provides the capability for authorized users to capture/record and log content related to a user session.

(3) *SESSION AUDIT | REMOTE VIEWING / LISTENING*

The information system provides the capability for authorized users to remotely view/hear all content related to an established user session in real time.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

AU-15 ALTERNATE AUDIT CAPABILITY

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

Supplemental Guidance: Since an alternate audit capability may be a short-term protection employed until the failure in the primary auditing capability is corrected, organizations may determine that the alternate audit capability need only provide a subset of the primary audit functionality that is impacted by the failure. Related control: AU-5.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

AU-16 CROSS-ORGANIZATIONAL AUDITING

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

Supplemental Guidance: When organizations use information systems and/or services of external organizations, the auditing capability necessitates a coordinated approach across organizations. For example, maintaining the identity of individuals that requested particular services across organizational boundaries may often be very difficult, and doing so may prove to have significant performance ramifications. Therefore, it is often the case that cross-organizational auditing (e.g., the type of auditing capability provided by service-oriented architectures) simply captures the identity of individuals issuing requests at the initial information system, and subsequent systems record that the requests emanated from authorized individuals. Related control: AU-6.

Control Enhancements:

(1) *CROSS-ORGANIZATIONAL AUDITING | IDENTITY PRESERVATION*

The organization requires that the identity of individuals be preserved in cross-organizational audit trails.

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

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

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

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

Moved (insertion) [5]

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

Deleted: ¶
Section Break (Next Page)

FAMILY: SECURITY ASSESSMENT AND AUTHORIZATION

CA-1 SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and

b. Reviews and updates the current:

1. Security assessment and authorization policy [*Assignment: organization-defined frequency*]; and

2. Security assessment and authorization procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the CA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-37, 800-53A, 800-100.

Priority and Baseline Allocation:

P1	**LOW** CA-1	**MOD** CA-1	**HIGH** CA-1

CA-2 SECURITY ASSESSMENTS

Control: The organization:

a. Develops a security assessment plan that describes the scope of the assessment including:

1. Security controls and control enhancements under assessment;

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

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

b. Assesses the security controls in the information system and its environment of operation [*Assignment: organization-defined frequency*] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements;

c. Produces a security assessment report that documents the results of the assessment; and

Deleted: CLASS: MANAGEMENT

Deleted: POLICIES

Deleted: develops,

Deleted: , and reviews/updates

Deleted: *frequency*

Deleted: Formal, documented

Deleted: policies

Deleted: address

Deleted: Formal, documented procedures

Deleted: policies

Deleted: .

Deleted: is intended to produce

Deleted: that are required

Deleted: security assessment and authorization

Deleted: The policies

Deleted: are consistent with

Deleted: policies,

Deleted: Existing organizational

Deleted: additional

Deleted: The security assessment/authorization policies

Deleted: the organization. Security assessment/authorization

Deleted: developed

Deleted: a

Deleted: system, when required.

Deleted: the development of the security assessment and authorization policy.

Deleted: the

Deleted: for the system

d. Provides the results of the security control assessment to [*Assignment: organization-defined individuals or roles*].

Supplemental Guidance: Organizations assess security controls in organizational information systems and the environments in which those systems operate as part of: (i) initial and ongoing security authorizations; (ii) FISMA annual assessments; (iii) continuous monitoring; and (iv) system development life cycle activities. Security assessments: (i) ensure that information security is built into organizational information systems; (ii) identify weaknesses and deficiencies early in the development process; (iii) provide essential information needed to make risk-based decisions as part of security authorization processes; and (iv) ensure compliance to vulnerability mitigation procedures. Assessments are conducted on the implemented security controls from Appendix F (main catalog) and Appendix G (Program Management controls) as documented in System Security Plans and Information Security Program Plans. Organizations can use other types of assessment activities such as vulnerability scanning and system monitoring to maintain the security posture of information systems during the entire life cycle. Security 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 security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements. The FISMA requirement for assessing security controls at least annually does not require additional assessment activities to those activities already in place in organizational security authorization processes. Security assessment results are provided to the individuals or roles appropriate for the types of assessments being conducted. For example, assessments conducted in support of security authorization decisions are provided to authorizing officials or authorizing official designated representatives.

To satisfy annual assessment requirements, organizations can use assessment results from the following sources: (i) initial or ongoing information system authorizations; (ii) continuous monitoring; or (iii) system development life cycle activities. Organizations ensure that security assessment results are current, relevant to the determination of security control effectiveness, and obtained with the appropriate level of assessor independence. Existing security 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.Subsequent to initial authorizations and in accordance with OMB policy, organizations assess security controls during continuous monitoring. Organizations establish the frequency for ongoing security control assessments in accordance with organizational continuous monitoring strategies. Information Assurance Vulnerability Alerts provide useful examples of vulnerability mitigation procedures. External audits (e.g., audits by external entities such as regulatory agencies) are outside the scope of this control. Related controls: CA-5, CA-6, CA-7, PM-9, RA-5, SA-11, SA-12, SI-4.

Control Enhancements:

(1) *SECURITY ASSESSMENTS | INDEPENDENT ASSESSORS*

The organization employs assessors or assessment teams with [*Assignment: organization-defined level of independence*] to conduct security control assessments.

Supplemental Guidance: Independent assessors or assessment teams are individuals or groups who conduct impartial assessments of organizational information systems. Impartiality implies that assessors are free from any perceived or actual conflicts of interest with regard to the development, operation, or management of the organizational information systems under assessment or to the determination of security control effectiveness. To achieve impartiality, assessors should not: (i) create a mutual or conflicting interest with the organizations where the assessments are being conducted; (ii) assess their own work; (iii) act as management or employees of the organizations they are serving; or (iv) 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 information systems and/or the ultimate risk to organizational operations, organizational assets, or individuals. Authorizing officials also determine if the level of assessor independence provides sufficient assurance that the results

Deleted: , in writing,…to the authorizing ...

Deleted: The organization assesses the ...

Deleted: the FISMA …nnual assessment ...

Deleted: an independent

Deleted: Enhancement …upplemental ...

are sound and can be used to make credible, risk-based decisions. This includes determining whether contracted security assessment services have sufficient independence, for example, when information system owners are not directly involved in contracting processes or cannot unduly influence the impartiality of assessors conducting assessments. In special situations, for example, when organizations that own the information 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.

(2) *SECURITY ASSESSMENTS | SPECIALIZED ASSESSMENTS*

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

Supplemental Guidance: Organizations can employ information system monitoring, insider threat assessments, malicious user testing, and other forms of testing (e.g., verification and validation) to improve readiness by exercising organizational capabilities and indicating current performance levels as a means of focusing actions to improve security. Organizations conduct assessment activities in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. Authorizing officials approve the assessment methods in coordination with the organizational risk executive function. Organizations can incorporate vulnerabilities uncovered during assessments into vulnerability remediation processes. Related controls: PE-3, SI-2.

(3) *SECURITY ASSESSMENTS | EXTERNAL ORGANIZATIONS*

The organization accepts the results of an assessment of [*Assignment: organization-defined information system*] performed by [*Assignment: organization-defined external organization*] when the assessment meets [*Assignment: organization-defined requirements*].

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

References: Executive Order 13587; FIPS Publication 199; NIST Special Publications 800-37, 800-39, 800-53A, 800-115, 800-137.

Priority and Baseline Allocation:

P2	**LOW** CA-2	**MOD** CA-2 (1)	**HIGH** CA-2 (1) (2)

CA-3 SYSTEM INTERCONNECTIONS

Control: The organization:

a. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements;

Deleted: produced

Deleted: a

Deleted: decision.

Deleted: the organization

Deleted: owns

Deleted: system is

Deleted: the

Deleted: structure requires

Deleted: the assessment be accomplished by individuals that

Deleted: and/

Deleted: the

Deleted: owner

Deleted: the

Deleted: process

Deleted: the

Deleted: an

Deleted: team

Deleted: *:*

Deleted: ***penetration***

Deleted: ***red team exercises;***

Deleted: ***testing***

Deleted: Enhancement

Deleted: Penetration testing exercises both physical and technical security controls. A standard method for penetration testing consi ...

Deleted: and organization. While penetrati ...

Deleted: penetration testing, red-team ...

Deleted: security

Deleted: independent

Deleted: are conducted

Deleted: the

Deleted: of the organization

Deleted: organizational

Deleted: the security state of the system an ...

Deleted: Testing methods are approved by ...

Deleted: organization's Risk Executive ...

Deleted: red team exercises are incorporated

Deleted: the

Deleted: process.

Deleted: RA-5

Deleted: INFORMATION

Deleted: CONNECTIONS

Deleted: outside of the authorization boundary

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

Deleted: connection

c. Reviews and updates Interconnection Security Agreements [*Assignment: organization-defined frequency*].

Deleted: <#>Monitors the information system connections on an ongoing basis verifying enforcement of security requirements.¶

Supplemental Guidance: This control applies to dedicated connections between information systems (i.e., system interconnections) and does not apply to transitory, user-controlled connections such as email and website browsing. Organizations carefully consider the risks that may be introduced when information systems are connected to other systems with different security requirements and security controls, both within organizations and external to organizations. Authorizing officials determine the risk associated with information 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, organizations can describe the interface characteristics between those interconnecting systems in their respective security plans. If interconnecting systems have different authorizing officials within the same organization, organizations can either develop Interconnection Security Agreements or describe the interface characteristics between systems in the security plans for the respective systems. Organizations may also incorporate Interconnection Security Agreement information into formal contracts, especially for interconnections established between federal agencies and nonfederal (i.e., private sector) organizations. Risk considerations also include information systems sharing the same networks. For certain technologies (e.g., space, unmanned aerial vehicles, and medical devices), there may be specialized connections in place during preoperational testing. Such connections may require Interconnection Security Agreements and be subject to additional security controls. Related controls: AC-3, AC-4, AC-20, AU-2, AU-12, AU-16, CA-7, IA-3, SA-9, SC-7, SI-4.

Deleted: The organization…rganizations ...

Control Enhancements:

(1) *SYSTEM INTERCONNECTIONS | UNCLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS*

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

Deleted: to an external network.¶
Enhancement Supplemental Guidance: An external network is a network that is not controlled by the organization (e.g., the Internet). No direct connection means that an information system cannot connect**… to an** ...

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

(2) *SYSTEM INTERCONNECTIONS | CLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS*

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

Deleted: .

Supplemental Guidance: Organizations typically do not have control over external networks (e.g., the Internet). Approved boundary protection devices (e.g., routers, firewalls) mediate communications (i.e., 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 information systems to external networks.

Deleted: Enhancement …upplemental ...

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

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

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

(4) *SYSTEM INTERCONNECTIONS | CONNECTIONS TO PUBLIC NETWORKS*

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

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

Deleted: AC-4

(5) SYSTEM INTERCONNECTIONS | RESTRICTIONS ON EXTERNAL SYSTEM CONNECTIONS

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

Supplemental Guidance: Organizations can constrain information system connectivity to external domains (e.g., websites) by employing one of two policies with regard to such connectivity: (i) allow-all, deny by exception, also known as *blacklisting* (the weaker of the two policies); or (ii) deny-all, allow by exception, also known as *whitelisting* (the stronger of the two policies). For either policy, organizations determine what exceptions, if any, are acceptable. Related control: CM-7.

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

Priority and Baseline Allocation:

P1	**LOW** CA-3	**MOD** CA-3 (5)	**HIGH** CA-3 (5)

CA-4 SECURITY CERTIFICATION

[Withdrawn: Incorporated into CA-2].

CA-5 PLAN OF ACTION AND MILESTONES

Control: The organization:

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

b. Updates existing plan of action and milestones [*Assignment: organization-defined frequency*] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

Supplemental Guidance: Plans of action and milestones are key documents in security authorization packages and are subject to federal reporting requirements established by OMB. Related controls: CA-2, CA-7, CM-4, PM-4.

Deleted: The plan

Deleted: is a

Deleted: document

Deleted: the

Deleted: package

Deleted: is

Deleted:

Deleted: control:

Control Enhancements:

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

The organization employs automated mechanisms to help ensure that the plan of action and milestones for the information system is accurate, up to date, and readily available.

References: OMB Memorandum 02-01; NIST Special Publication 800-37.

Priority and Baseline Allocation:

P3	**LOW** CA-5	**MOD** CA-5	**HIGH** CA-5

CA-6 SECURITY AUTHORIZATION

Control: The organization:

a. Assigns a senior-level executive or manager as the authorizing official for the information system;

Deleted: to…s the role of ...

b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and

c. Updates the security authorization [*Assignment: organization-defined frequency*].

Supplemental Guidance: Security authorizations are official management decisions, conveyed through authorization decision documents, by senior organizational officials or executives (i.e., authorizing officials) to authorize operation of information 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 controls. Authorizing officials provide budgetary oversight for organizational information systems or assume responsibility for the mission/business operations supported by those systems. The security authorization process is an inherently federal responsibility and therefore, authorizing officials must be federal employees. Through the security authorization process, authorizing officials assume responsibility and are accountable for security risks associated with the operation and use of organizational information systems. Accordingly, authorizing officials are in positions with levels of authority commensurate with understanding and accepting such information security-related risks. OMB policy requires that organizations conduct ongoing authorizations of information systems by implementing continuous monitoring programs. Continuous monitoring programs can satisfy three-year reauthorization requirements, so separate reauthorization processes are not necessary. Through the employment of comprehensive continuous monitoring processes, critical information contained in authorization packages (i.e., security plans, security assessment reports, and plans of action and milestones) is updated on an ongoing basis, providing authorizing officials and information system owners with an up-to-date status of the security state of organizational information systems and environments of operation. To reduce the administrative cost of security reauthorization, authorizing officials use the results of continuous monitoring processes to the maximum extent possible as the basis for rendering reauthorization decisions. Related controls: CA-2, CA-7, PM-9, PM-10.

Deleted: authorization is the …uthorizations ...

Control Enhancements: None.

References: OMB Circular A-130; OMB Memorandum 11-33; NIST Special Publications 800-37, 800-137.

Priority and Baseline Allocation:

P2	**LOW** CA-6	**MOD** CA-6	**HIGH** CA-6

Deleted: P3

CA-7 CONTINUOUS MONITORING

Control: The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:

Deleted: establishes

a. Establishment of [*Assignment: organization-defined metrics*] to be monitored;

b. Establishment of [*Assignment: organization-defined frequencies*] for monitoring and [*Assignment: organization-defined frequencies*] for assessments supporting such monitoring;

Deleted: <#>A configuration management process for the information system and its constituent components;¶
<#>A determination of the security impact of changes to the information system and environment of operation;¶

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

Deleted: and

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

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

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

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

Supplemental Guidance: Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. The terms *continuous* and *ongoing* imply that organizations assess/analyze security controls and information security-related risks at a frequency sufficient to support organizational risk-based decisions. The results of continuous monitoring programs generate appropriate risk response actions by organizations. Continuous monitoring programs also allow organizations to maintain the security authorizations of information systems and common controls over time in highly dynamic environments of operation with changing mission/business needs, threats, vulnerabilities, and technologies. Having access to security-related information on a continuing basis through reports/dashboards gives organizational officials the capability to make more effective and timely risk management decisions, including ongoing security authorization decisions. Automation supports more frequent updates to security authorization packages, hardware/software/firmware inventories, 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 information systems. Related controls: CA-2, CA-5, CA-6, CM-3, CM-4, PM-6, PM-9, RA-5, SA-11, SA-12, SI-2, SI-4.

Control Enhancements:

(1) *CONTINUOUS MONITORING | INDEPENDENT ASSESSMENT*

The organization employs assessors or assessment teams with [*Assignment: organization-defined level of independence*] to monitor the security controls in the information system on an ongoing basis.

Supplemental Guidance: Organizations can maximize the value of assessments of security controls during the continuous monitoring process by requiring that such assessments be conducted by assessors or assessment teams with appropriate levels of independence based on continuous monitoring strategies. Assessor independence provides a degree of impartiality to the monitoring process. To achieve such impartiality, assessors should not: (i) create a mutual or conflicting interest with the organizations where the assessments are being conducted; (ii) assess their own work; (iii) act as management or employees of the organizations they are serving; or (iv) place themselves in advocacy positions for the organizations acquiring their services.

(2) *CONTINUOUS MONITORING | TYPES OF ASSESSMENTS*

[Withdrawn: Incorporated into CA-2.]

(3) *CONTINUOUS MONITORING | TREND ANALYSES*

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

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

References: OMB Memorandum 11-33; NIST Special Publications 800-37, 800-39, 800-53A, 800-115, 800-137; US-CERT Technical Cyber Security Alerts; DoD Information Assurance Vulnerability Alerts.

Priority and Baseline Allocation:

Deleted: state

Deleted: appropriate organizational officials

Deleted: A continuous monitoring program allows an organization to maintain the security authorization of an information system over time in a highly dynamic environment of operation with changing threats, vulnerabilities, technologies, and missions/business processes.

Deleted: of security controls using automated support tools facilitates near real-time risk management and promotes organizational situational

Deleted: with regard to the

Deleted: state of the information system.

Deleted: implementation of a

Deleted: monitoring program results in ongoing updates to the security plan, the security assessment report, and the plan of action

Deleted: milestones, the three principal documents in the security authorization package. A rigorous and well executed

Deleted: program significantly reduces the level of effort required for the reauthorization of the

Deleted: system.

Deleted: impact level

Deleted: the

Deleted: system.

Deleted: .

Deleted: an independent assessor

Deleted: team

Deleted: Enhancement

Deleted: The organization

Deleted: extend and

Deleted: the ongoing assessment

Deleted: an independent assessor or team to assess all

Deleted: the security controls during the information system's three-year authorization cycle. See supplemental guidance for CA-2, enhancement (1), for further information on assessor independence. Related controls: CA-2, CA-5, CA-6, CM-4

Deleted: The organization plans, schedules, and conducts assessments [*Assignment: organization-defined frequency*], [*Selection: announced; unannounced*], [*Selection: in-depth monitoring; malicious user testing; penetration testing; red team exercises;* [*Assignment: organization-defined oth

...

Deleted: Enhancement Supplemental Guidance: Examples of vulnerability

...

Deleted: DOD

P2	**LOW** CA-7	**MOD** CA-7 (1)	**HIGH** CA-7 (1)

Deleted: P3

CA-8 PENETRATION TESTING

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

Supplemental Guidance: Penetration testing is a specialized type of assessment conducted on information systems or individual system components to identify vulnerabilities that could be exploited by adversaries. Such testing can be used to either validate vulnerabilities or determine the degree of resistance organizational information systems have to adversaries within a set of specified constraints (e.g., time, resources, and/or skills). Penetration testing attempts to duplicate the actions of adversaries in carrying out hostile cyber attacks against organizations and provides a more in-depth analysis of security-related weaknesses/deficiencies. Organizations can also use the results of vulnerability analyses to support penetration testing activities. Penetration testing can be conducted on the hardware, software, or firmware components of an information system and can exercise both physical and technical security controls. A standard method for penetration testing includes, for example: (i) pretest analysis based on full knowledge of the target system; (ii) pretest identification of potential vulnerabilities based on pretest analysis; and (iii) testing designed to determine exploitability of identified vulnerabilities. All parties agree to the rules of engagement before the commencement of penetration testing scenarios. Organizations correlate the penetration testing rules of engagement with the tools, techniques, and procedures that are anticipated to be employed by adversaries carrying out attacks. Organizational risk assessments guide decisions on the level of independence required for personnel conducting penetration testing. Related control: SA-12.

Control Enhancements:

(1) *PENETRATION TESTING | INDEPENDENT PENETRATION AGENT OR TEAM*

The organization employs an independent penetration agent or penetration team to perform penetration testing on the information system or system components.

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

(2) *PENETRATION TESTING | RED TEAM EXERCISES*

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

Supplemental Guidance: Red team exercises extend the objectives of penetration testing by examining the security posture of organizations and their ability to implement effective cyber defenses. As such, red team exercises reflect simulated adversarial attempts to compromise organizational mission/business functions and provide a comprehensive assessment of the security state of information systems and organizations. Simulated adversarial attempts to compromise organizational missions/business functions and the information systems that support those missions/functions may include technology-focused attacks (e.g., interactions with hardware, software, or firmware components and/or mission/business processes) and social engineering-based attacks (e.g., interactions via email, telephone, shoulder surfing, or personal conversations). While penetration testing may be largely laboratory-based testing, organizations use red team exercises to provide more comprehensive assessments that reflect real-world conditions. Red team exercises can be used to improve security awareness and training and to assess levels of security control effectiveness.

References: None.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** Not Selected	**HIGH** CA-8

CA-9 INTERNAL SYSTEM CONNECTIONS

Control: The organization:

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

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

Supplemental Guidance: This control applies to connections between organizational information systems and (separate) constituent system components (i.e., intra-system connections) including, for example, system connections with mobile devices, notebook/desktop computers, printers, copiers, facsimile machines, scanners, sensors, and servers. Instead of authorizing each individual internal connection, organizations can authorize internal connections for a class of components with common characteristics and/or configurations, for example, all digital printers, scanners, and copiers with a specified processing, storage, and transmission capability or all smart phones with a specific baseline configuration. Related controls: AC-3, AC-4, AC-18, AC-19, AU-2, AU-12, CA-7, CM-2, IA-3, SC-7, SI-4.

Control Enhancements:

(1) *INTERNAL SYSTEM CONNECTIONS | SECURITY COMPLIANCE CHECKS*

The information system performs security compliance checks on constituent system components prior to the establishment of the internal connection.

Supplemental Guidance: Security compliance checks may include, for example, verification of the relevant baseline configuration. Related controls: CM-6.

References: None.

Priority and Baseline Allocation:

P2	**LOW** CA-9	**MOD** CA-9	**HIGH** CA-9

FAMILY: CONFIGURATION MANAGEMENT

Deleted:
CLASS: OPERATIONAL

CM-1 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES

Control: The organization:

Deleted: develops,

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

Deleted: , and reviews/updates…to …

1. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

Deleted: A formal, documented

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

Deleted: Formal, documented …

b. Reviews and updates the current:

1. Configuration management policy [*Assignment: organization-defined frequency*]; and

2. Configuration management procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the CM family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Deleted: is intended to produce…ddresses th …

Control Enhancements: None.

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

Priority and Baseline Allocation:

P1	**LOW** CM-1	**MOD** CM-1	**HIGH** CM-1

CM-2 BASELINE CONFIGURATION

Control: The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

Supplemental Guidance: This control establishes baseline configurations for information 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 information systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, and/or changes to information systems. Baseline configurations include information about information system components (e.g., standard software packages installed on workstations, notebook computers, servers, network components, or mobile devices; current version numbers and patch information on operating systems and applications; and configuration settings/parameters), network topology, and the logical placement of those components within the system architecture. Maintaining baseline configurations requires creating new baselines as organizational information systems change over time. Baseline configurations of information systems reflect the current enterprise architecture. Related controls: CM-3, CM-6, CM-8, CM-9, SA-10, PM-5, PM-7.

Deleted: a …aseline configuration …

Control Enhancements:

(1) *BASELINE CONFIGURATION | REVIEWS AND UPDATES*

The organization reviews and updates the baseline configuration of the information system:

(a) [*Assignment: organization-defined frequency*];

(b) When required due to [*Assignment organization-defined circumstances*]; and

(c) As an integral part of information system component installations and upgrades.

Supplemental Guidance: Related control: CM-5.

(2) *BASELINE CONFIGURATION | AUTOMATION SUPPORT FOR ACCURACY / CURRENCY*

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

Supplemental Guidance: Automated mechanisms that help organizations maintain consistent baseline configurations for information 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 information system level, or at the operating system or component level (e.g., on workstations, servers, notebook computers, network components, or mobile devices). Tools can be used, for example, to track version numbers on operating system 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 information system component inventory and baseline configuration activities. Related controls: CM-7, RA-5.

(3) *BASELINE CONFIGURATION | RETENTION OF PREVIOUS CONFIGURATIONS*

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

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

(4) *BASELINE CONFIGURATION | UNAUTHORIZED SOFTWARE*

[Withdrawn: Incorporated into CM-7].

(5) *BASELINE CONFIGURATION | AUTHORIZED SOFTWARE*

[Withdrawn: Incorporated into CM-7].

(6) *BASELINE CONFIGURATION | DEVELOPMENT AND TEST ENVIRONMENTS*

The organization maintains a baseline configuration for information system development and test environments that is managed separately from the operational baseline configuration.

Supplemental Guidance: Establishing separate baseline configurations for development, testing, and operational environments helps protect information systems from unplanned/unexpected events related to development and testing activities. Separate baseline configurations allow organizations to apply the configuration management that is most appropriate for each type of configuration. For example, management of operational configurations typically emphasizes the need for stability, while management of development/test configurations requires greater flexibility. Configurations in the test environment mirror the configurations in the operational environment to the extent practicable so that the results of the testing are representative of the proposed changes to the operational systems. This control enhancement requires separate configurations but not necessarily separate physical environments. Related controls: CM-4, SC-3, SC-7.

(7) *BASELINE CONFIGURATION | CONFIGURE SYSTEMS, COMPONENTS, OR DEVICES FOR HIGH-RISK AREAS*

The organization:

Deleted: Enhancement

Deleted: Software inventory tools are examples of automated

Deleted: . Software inventory

Deleted: for each operating

Deleted: in use within the organization

Deleted:) and

Deleted: version numbers,

Deleted: and

Deleted: on the operating systems

Deleted: Software inventory tools can also scan information systems for unauthorized software to validate organization-defined lists

Deleted: older

Deleted: as deemed necessary

Deleted: The organization:¶
Develops and [*Assignment: organization-defined list of software programs not authorized to execute on the information system*]; and

Deleted: Employs an allow-all, deny-by-exception authorization policy to identify software allowed to execute on the information system

Deleted: The organization:¶
<#>Develops and maintains [*Assignment: organization-defined list of software programs authorized to execute on the information system*]; and¶
Employs a deny-all, permit-by-exception authorization policy to identify software allowed to execute on the

Deleted: information system.

(a) Issues [*Assignment: organization-defined information systems, system components, or devices*] with [*Assignment: organization-defined configurations*] to individuals traveling to locations that the organization deems to be of significant risk; and

(b) Applies [*Assignment: organization-defined security safeguards*] to the devices when the individuals return.

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

References: NIST Special Publication 800-128.

Priority and Baseline Allocation:

P1	**LOW** CM-2	**MOD** CM-2 (1) (3) (7)	**HIGH** CM-2 (1) (2) (3) (7)

CM-3 CONFIGURATION CHANGE CONTROL

Control: The organization:

a. Determines the types of changes to the information system that are configuration-controlled;

b. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses;

c. Documents configuration change decisions associated with the information system;

d. Implements approved configuration-controlled changes to the information system;

e. Retains records of configuration-controlled changes to the information system for [*Assignment: organization-defined time period*];

f. Audits and reviews activities associated with configuration-controlled changes to the information system; and

g. Coordinates and provides oversight for configuration change control activities through [*Assignment: organization-defined configuration change control element (e.g., committee, board*] that convenes [*Selection (one or more):* [*Assignment: organization-defined frequency*]; [*Assignment: organization-defined configuration change conditions*]].

Supplemental Guidance: Configuration change controls for organizational information 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 information systems, changes to configuration settings for information technology products (e.g., operating systems, applications, firewalls, routers, and mobile devices), unscheduled/unauthorized changes, and changes to remediate vulnerabilities. Typical processes for managing configuration changes to information systems include, for example, Configuration Control Boards that approve proposed changes to systems. For new development information systems or systems undergoing

Deleted: (4)

Deleted: 5) (6

Deleted: Approves

Deleted: and reviews

Deleted: system;

Deleted: :

Deleted: The organization determines the types of changes to the information system that are configuration controlled.

Deleted: control

Deleted: the

Deleted: system involves

Deleted: test/evaluation

Deleted: system

Deleted:

Deleted: the

Deleted: system

Deleted: the

Deleted:), emergency

Deleted: flaws. A typical organizational process

Deleted: the

Deleted: system includes

Deleted: a chartered

Deleted: Board

Deleted: approves

Deleted: the system.

major upgrades, organizations consider including representatives from development organizations on the Configuration Control Boards. Auditing of changes includes activities before and after changes are made to organizational information systems and the auditing activities required to implement such changes. Related controls: CM-2, CM-4, CM-5, CM-6, CM-9, SA-10, SI-2, SI-12.

Control Enhancements:

(1) *CONFIGURATION CHANGE CONTROL | AUTOMATED DOCUMENT / NOTIFICATION / PROHIBITION OF CHANGES*

The organization employs automated mechanisms to:

(a) Document proposed changes to the information system;

(b) Notify [*Assignment: organized-defined approval authorities*] of proposed changes to the information system and request change approval;

(c) Highlight proposed changes to the information system that have not been approved or disapproved by [*Assignment: organization-defined time period*];

(d) Prohibit changes to the information system until designated approvals are received;

(e) Document all changes to the information system; and

(f) Notify [*Assignment: organization-defined personnel*] when approved changes to the information system are completed.

(2) *CONFIGURATION CHANGE CONTROL | TEST / VALIDATE / DOCUMENT CHANGES*

The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.

Supplemental Guidance: Changes to information systems include modifications to hardware, software, or firmware components and configuration settings defined in CM-6. Organizations ensure that testing does not interfere with information system operations. Individuals/groups conducting tests understand organizational security policies and procedures, information system security policies and procedures, and the specific health, safety, and environmental risks associated with particular facilities/processes. Operational systems may need to be taken off-line, or replicated to the extent feasible, before testing can be conducted. If information systems must be taken off-line for testing, the tests are scheduled to occur during planned system outages whenever possible. If testing cannot be conducted on operational systems, organizations employ compensating controls (e.g., testing on replicated systems).

(3) *CONFIGURATION CHANGE CONTROL | AUTOMATED CHANGE IMPLEMENTATION*

The organization employs automated mechanisms to implement changes to the current information system baseline and deploys the updated baseline across the installed base.

(4) *CONFIGURATION CHANGE CONTROL | SECURITY REPRESENTATIVE*

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

Supplemental Guidance: Information security representatives can include, for example, senior agency information security officers, information system security officers, or information system security managers. Representation by personnel with information security expertise is important because changes to information 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 information systems. The configuration change control element in this control enhancement reflects the change control elements defined by organizations in CM-3.

(5) *CONFIGURATION CHANGE CONTROL | AUTOMATED SECURITY RESPONSE*

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

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

(6) *CONFIGURATION CHANGE CONTROL | CRYPTOGRAPHY MANAGEMENT*

Deleted: refers to changes in activity

Deleted: a change is

Deleted: the

Deleted: system

Deleted: the change.

Deleted: designated

Deleted: approvals

Deleted: received

Deleted: Inhibit change

Deleted: and

Deleted: changes to the information system

Deleted: Enhancement

Deleted: The organization ensures

Deleted: The individual/group

Deleted: the

Deleted: understands the

Deleted: information

Deleted: the

Deleted: a

Deleted: facility and/or process. An operational system

Deleted:

Deleted: an

Deleted: system

Deleted: In situations where the organization cannot conduct

Deleted: of an

Deleted: system, the organization employs

Deleted: providing a

Deleted: system to conduct testing) in accordance with the general tailoring guidance.

Deleted: Enhancement Supplemental Guidance: Related controls: CM-2, CM-6.¶

Deleted: *(e.g., committee, board)*].

Deleted: Enhancement

Deleted: is consistent with

Deleted: element

Deleted: the

Deleted: in CM-3

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

Supplemental Guidance: Regardless of the cryptographic means employed (e.g., public key, private key, shared secrets), organizations ensure that there are processes and procedures in place to effectively manage those means. For example, if devices use certificates as a basis for identification and authentication, there needs to be a process in place to address the expiration of those certificates. Related control: SC-13.

References: NIST Special Publication 800-128.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** CM-3 (2)	**HIGH** CM-3 (1) (2)

CM-4 SECURITY IMPACT ANALYSIS

Control: The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.

Supplemental Guidance: Organizational personnel with information security responsibilities (e.g., Information System Administrators, Information System Security Officers, Information System Security Managers, and Information System Security Engineers) conduct security impact analyses. Individuals conducting security impact analyses possess the necessary skills/technical expertise to analyze the changes to information systems and the associated security ramifications. Security impact analysis may include, for example, reviewing security plans to understand security control requirements and reviewing system design documentation to understand control implementation and how specific changes might affect the controls. Security impact analyses may also include assessments of risk to better understand the impact of the changes and to determine if additional security controls are required. Security impact analyses are scaled in accordance with the security categories of the information systems. Related controls: CA-2, CA-7, CM-3, CM-9, SA-4, SA-5, SA-10, SI-2.

Control Enhancements:

(1) *SECURITY IMPACT ANALYSIS | SEPARATE TEST ENVIRONMENTS*

The organization analyzes changes to the information system in a separate test environment before implementation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.

Supplemental Guidance: Separate test environment in this context means an environment that is physically or logically isolated and distinct from the operational environment. The separation is sufficient to ensure that activities in the test environment do not impact activities in the operational environment, and information in the operational environment is not inadvertently transmitted to the test environment. Separate environments can be achieved by physical or logical means. If physically separate test environments are not used, organizations determine the strength of mechanism required when implementing logical separation (e.g., separation achieved through virtual machines). Related controls: SA-11, SC-3, SC-7.

(2) *SECURITY IMPACT ANALYSIS | VERIFICATION OF SECURITY FUNCTIONS*

The organization, after the information system is changed, checks the security functions to verify that the functions are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security requirements for the system.

Supplemental Guidance: Implementation is this context refers to installing changed code in the operational information system. Related control: SA-11.

References: NIST Special Publication 800-128.

Priority and Baseline Allocation:

Deleted: Security impact analyses are conducted by organizational

Deleted: , including for example,

Deleted: .

Deleted: have

Deleted: appropriate

Deleted: and

Deleted:

Deleted: information

Deleted: such as the security plan to understand how specific security controls are implemented within the system

Deleted: the

Deleted:

Deleted: analysis

Deleted: an assessment

Deleted:

Deleted: analysis is

Deleted: impact level

Deleted: system.

Deleted: new software

Deleted: installation

Deleted: Enhancement

Deleted: Changes include

Deleted: upgrades and modifications

P2	**LOW** CM-4	**MOD** CM-4	**HIGH** CM-4 (1)

CM-5 ACCESS RESTRICTIONS FOR CHANGE

Control: The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.

Supplemental Guidance: Any changes to the hardware, software, and/or firmware components of information systems can potentially have significant effects on the overall security of the systems. Therefore, organizations permit only qualified and authorized individuals to access information systems for purposes of initiating changes, including upgrades and modifications. Organizations maintain records of access to ensure that configuration change control is implemented and to support after-the-fact actions should organizations discover any unauthorized changes. Access restrictions for change also include software libraries. Access restrictions include, for example, physical and logical access controls (see AC-3 and PE-3), workflow automation, media libraries, abstract layers (e.g., changes implemented into third-party interfaces rather than directly into information systems), and change windows (e.g., changes occur only during specified times, making unauthorized changes easy to discover). Related controls: AC-3, AC-6, PE-3.

Control Enhancements:

(1) *ACCESS RESTRICTIONS FOR CHANGE | AUTOMATED ACCESS ENFORCEMENT / AUDITING*

The information system enforces access restrictions and supports auditing of the enforcement actions.

Supplemental Guidance: Related controls: AU-2, AU-12, AU-6, CM-3, CM-6.

(2) *ACCESS RESTRICTIONS FOR CHANGE | REVIEW SYSTEM CHANGES*

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

Supplemental Guidance: Indications that warrant review of information system changes and the specific circumstances justifying such reviews may be obtained from activities carried out by organizations during the configuration change process. Related controls: AU-6, AU-7, CM-3, CM-5, PE-6, PE-8.

(3) *ACCESS RESTRICTIONS FOR CHANGE | SIGNED COMPONENTS*

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

Supplemental Guidance: Software and firmware components prevented from installation unless signed with recognized and approved certificates include, for example, software and firmware version updates, patches, service packs, device drivers, and basic input output system (BIOS) updates. Organizations can identify applicable software and firmware components by type, by specific items, or a combination of both. Digital signatures and organizational verification of such signatures, is a method of code authentication. Related controls: CM-7, SC-13, SI-7.

(4) *ACCESS RESTRICTIONS FOR CHANGE | DUAL AUTHORIZATION*

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

Supplemental Guidance: Organizations employ dual authorization to ensure that any changes to selected information system components and information cannot occur unless two qualified individuals implement such changes. The two individuals possess sufficient skills/expertise to determine if the proposed changes are correct implementations of approved changes. Related controls: AC-5, CM-3.

(5) *ACCESS RESTRICTIONS FOR CHANGE | LIMIT PRODUCTION / OPERATIONAL PRIVILEGES*

The organization:

(a) Limits privileges to change information system components and system-related information within a production or operational environment; and

Deleted: the

Deleted: system

Deleted: system. Accordingly,

Deleted: are allowed to obtain

Deleted: to

Deleted: system components

Deleted: Additionally, maintaining

Deleted: is essential for ensuring

Deleted: being

Deleted: as intended

Deleted: for supporting

Deleted: the organization become aware of an

Deleted: change to the information system.

Deleted: Examples of access

Deleted: are

Deleted: a

Deleted: interface

Deleted: the

Deleted: system component

Deleted: outside the window

Deleted: Some or all of the enforcement mechanisms and processes necessary to implement this security control are included in other controls. For measures implemented in other controls, this control provides information to be used in the implementation of the other controls to cover specific needs related to enforcing authorizations to make changes to the information system, auditing changes, and retaining and review records of changes.

Deleted: The organization employs

Deleted: automated mechanisms to ...

Deleted: conducts audits of

Deleted: when indications so warrant

Deleted: *critical*

Deleted: *programs*]

Deleted: are not

Deleted: with

Deleted: Enhancement

Deleted: Critical software programs

Deleted: /or modules

Deleted: and where applicable,

Deleted: a two-person rule for

Deleted: information system ...

Deleted: hardware, software, and ...

Deleted: directly

(b) Reviews and reevaluates privileges [*Assignment: organization-defined frequency*].

Supplemental Guidance: In many organizations, information systems support multiple core missions/business functions. Limiting privileges to change information system components with respect to operational systems is necessary because changes to a particular information system component may have far-reaching effects on mission/business processes supported by the system where the component resides. The complex, many-to-many relationships between systems and mission/business processes are in some cases, unknown to developers. Related control: AC-2.

(6) *ACCESS RESTRICTIONS FOR CHANGE | LIMIT LIBRARY PRIVILEGES*

The organization limits privileges to change software resident within software libraries.

Supplemental Guidance: Software libraries include privileged programs. Related control: AC-2.

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

[Withdrawn: Incorporated into SI-7].

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** CM-5	**HIGH** CM-5 (1) (2) (3)

CM-6 CONFIGURATION SETTINGS

Control: The organization:

a. Establishes and documents configuration settings for information technology products employed within the information system using [*Assignment: organization-defined security configuration checklists*] that reflect the most restrictive mode consistent with operational requirements;

b. Implements the configuration settings;

c. Identifies, documents, and approves any deviations from established configuration settings for [*Assignment: organization-defined information system components*] based on [*Assignment: organization-defined operational requirements*]; and

d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

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

Deleted: information system developer/integrator

Deleted: (including

Deleted:).

Deleted: The information system automatically implements [*Assignment: organization-defined safeguards and countermeasures*] if security functions (or mechanisms) are changed inappropriately.¶
Enhancement Supplemental Guidance: The information system reacts automatically when inappropriate and/or unauthorized modifications have occurred to security functions or mechanisms. Automatic implementation of safeguards and countermeasures includes, for example, reversing the change, halting the information system or triggering an audit alert when an unauthorized modification to a critical security file occurs.¶

Deleted: mandatory

Deleted: exceptions

Deleted: the mandatory

Deleted: individual components within the

Deleted: explicit

Deleted: ;

Deleted: configurable security-related

Deleted: of information

Deleted: that are part of the information system.

Deleted: the system

Deleted: related

Deleted: meeting

Deleted:

Deleted: ,

Deleted: and

Deleted: settings (i.e., permissions); and

Deleted: services

Deleted:

Deleted: mandatory configuration settings from which the settings for a given information system are derived. A *security*

Deleted: *checklist* (sometimes

Deleted: a

Deleted: guide,

Deleted: guide

Deleted: guide

Deleted: guide [STIG], or benchmark) is a series of

Deleted: or procedures

Deleted: an

information 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. Common secure configurations include the United States Government Configuration Baseline (USGCB) which affects the implementation of CM-6 and other controls such as AC-19 and CM-7. The Security Content Automation Protocol (SCAP) and the defined standards within the protocol (e.g., Common Configuration Enumeration) provide an effective method to uniquely identify, track, and control configuration settings. OMB establishes federal policy on configuration requirements for federal information systems. Related controls: AC-19, CM-2, CM-3, CM-7, SI-4.

Control Enhancements:

(1) *CONFIGURATION SETTINGS | AUTOMATED CENTRAL MANAGEMENT / APPLICATION / VERIFICATION*

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

Supplemental Guidance: Related controls: CA-7, CM-4.

(2) *CONFIGURATION SETTINGS | RESPOND TO UNAUTHORIZED CHANGES*

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

Supplemental Guidance: Responses to unauthorized changes to configuration settings can include, for example, alerting designated organizational personnel, restoring established configuration settings, or in extreme cases, halting affected information system processing. Related controls: IR-4, SI-7.

(3) *CONFIGURATION SETTINGS | UNAUTHORIZED CHANGE DETECTION*

[Withdrawn: Incorporated into SI-7].

(4) *CONFIGURATION SETTINGS | CONFORMANCE DEMONSTRATION*

[Withdrawn: Incorporated into CM-4].

References: OMB Memoranda 07-11, 07-18, 08-22; NIST Special Publications 800-70, 800-128; Web: nvd.nist.gov, checklists.nist.gov, www.nsa.gov.

Priority and Baseline Allocation:

P1	**LOW** CM-6	**MOD** CM-6	**HIGH** CM-6 (1) (2)

CM-7 LEAST FUNCTIONALITY

Control: The organization:

a. Configures the information system to provide only essential capabilities; and

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

Supplemental Guidance: Information systems can provide a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions). Additionally, it is sometimes convenient to provide multiple services from single information system components, but doing so increases risk over limiting the services provided by any one component. Where feasible, organizations limit component functionality to a single function per device (e.g., email servers or web servers, but not both). Organizations review functions and services provided by information systems or individual components of information systems, to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol, Instant Messaging, auto-execute, and file sharing).

Deleted: component

Deleted: Checklists

Deleted: and

Deleted: (

Deleted: government

Deleted:), and others

Deleted: An example of a security configuration checklist is the Federal Desktop Core

Deleted: (FDCC

Deleted: potentially

Deleted:

Deleted:

Deleted:

Deleted:

Deleted: automated mechanisms

Deleted: Enhancement

Deleted: mandatory/organization-defined

Deleted: the

Deleted: case

Deleted: The organization incorporates detection of unauthorized, security-relevant configuration changes into the organization's incident response capability to ensure that such detected events are tracked, monitored, corrected, and available for historical purposes.¶ ...

Deleted: The information system ...

Deleted: ;

Deleted: (3)

Deleted: (3)

Deleted: configures

Deleted: specifically prohibits

Deleted: *list of*

Deleted: are capable of providing

Deleted:

Deleted:

Deleted: a

Deleted: component of an

Deleted:

Deleted: server

Deleted: server,

Deleted: The

Deleted: organizational

Deleted: ,

Deleted: are carefully reviewed

Organizations consider disabling unused or unnecessary physical and logical ports/protocols (e.g., Universal Serial Bus, File Transfer Protocol, and Hyper Text Transfer Protocol) on information systems to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling. Organizations can utilize network scanning tools, intrusion detection and prevention systems, and end-point protections such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols, and services. Related controls: AC-6, CM-2, RA-5, SA-5, SC-7.

Control Enhancements:

(1) *LEAST FUNCTIONALITY | PERIODIC REVIEW*

The organization:

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

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

Supplemental Guidance: The organization can either make a determination of the relative security of the function, port, protocol, and/or service or base the security decision on the assessment of other entities. Bluetooth, FTP, and peer-to-peer networking are examples of less than secure protocols. Related controls: AC-18, CM-7, IA-2.

(2) *LEAST FUNCTIONALITY | PREVENT PROGRAM EXECUTION*

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

Supplemental Guidance: Related controls: CM-8, PM-5.

(3) *LEAST FUNCTIONALITY | REGISTRATION COMPLIANCE*

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

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

(4) *LEAST FUNCTIONALITY | UNAUTHORIZED SOFTWARE / BLACKLISTING*

The organization:

(a) Identifies [*Assignment: organization-defined software programs not authorized to execute on the information system*];

(b) Employs an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system; and

(c) Reviews and updates the list of unauthorized software programs [*Assignment: organization-defined frequency*].

Supplemental Guidance: The process used to identify software programs that are not authorized to execute on organizational information systems is commonly referred to as *blacklisting*. Organizations can implement CM-7 (5) instead of this control enhancement if whitelisting (the stronger of the two policies) is the preferred approach for restricting software program execution. Related controls: CM-6, CM-8, PM-5.

(5) *LEAST FUNCTIONALITY | AUTHORIZED SOFTWARE / WHITELISTING*

The organization:

(a) Identifies [*Assignment: organization-defined software programs authorized to execute on the information system*];

(b) Employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system; and

(c) Reviews and updates the list of authorized software programs [*Assignment: organization-defined frequency*].

Supplemental Guidance: The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as *whitelisting*. In

Deleted:

Deleted: and

Deleted: [USB],

Deleted: [FTP], Internet Protocol Version 6 [IPv6],

Deleted: [HTTP])

Deleted: system components

Deleted:

Deleted:

Deleted: control:

Deleted: and eliminate

Deleted: /or

Deleted: .

Deleted: The organization employs automated mechanisms

Deleted: ***list of authorized software programs; list of unauthorized software programs;***

Deleted: Enhancement

Deleted: 2

Deleted: Enhancement

Deleted: functionality

addition to whitelisting, organizations consider verifying the integrity of white-listed software programs using, for example, cryptographic checksums, digital signatures, or hash functions. Verification of white-listed software can occur either prior to execution or at system startup. Related controls: CM-2, CM-6, CM-8, PM-5, SA-10, SC-34, SI-7.

References: DoD Instruction 8551.01.

Priority and Baseline Allocation:

P1	**LOW** CM-7	**MOD** CM-7 (1) (2) (4)	**HIGH** CM-7 (1) (2) (5)

CM-8 INFORMATION SYSTEM COMPONENT INVENTORY

Control: The organization:

a. Develops and documents an inventory of information system components that:

1. Accurately reflects the current information system;
2. Includes all components within the authorization boundary of the information system;
3. Is at the level of granularity deemed necessary for tracking and reporting; and
4. Includes [*Assignment: organization-defined information deemed necessary to achieve effective information system component accountability*]; and

b. Reviews and updates the information system component inventory [*Assignment: organization-defined frequency*].

Supplemental Guidance: Organizations may choose to implement centralized information system component inventories that include components from all organizational information systems. In such situations, organizations ensure that the resulting inventories include system-specific information required for proper component accountability (e.g., information system association, information system owner). Information deemed necessary for effective accountability of information system components includes, for example, hardware inventory specifications, software license information, software version numbers, component owners, and for networked components or devices, machine names and network addresses. Inventory specifications include, for example, manufacturer, device type, model, serial number, and physical location. Related controls: CM-2, CM-6, PM-5.

Control Enhancements:

(1) *INFORMATION SYSTEM COMPONENT INVENTORY | UPDATES DURING INSTALLATIONS / REMOVALS*

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

(2) *INFORMATION SYSTEM COMPONENT INVENTORY | AUTOMATED MAINTENANCE*

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

Supplemental Guidance: Organizations maintain information 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 information system component inventory and baseline configuration activities. Related control: SI-7.

(3) *INFORMATION SYSTEM COMPONENT INVENTORY | AUTOMATED UNAUTHORIZED COMPONENT DETECTION*

The organization:

Deleted: develops

Deleted: , and maintains

Deleted: Is consistent with

Deleted: *property*

Deleted: <#>Is available for review and audit by designated organizational officials.¶

Deleted: to be

Deleted: by the organization to achieve

Deleted: property

Deleted: can include

Deleted: (

Deleted:), software license information, information system/component owner, and for a networked component/device, the machine name and network address

Deleted: Enhancement

Deleted: the

Deleted: inventory

Deleted: they

Deleted:

Deleted: the intent of this control enhancement is to

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

(b) Takes the following actions when unauthorized components are detected: [*Selection (one or more): disables* network access by such components*; isolates the components;* notifies *[Assignment: organization-defined personnel or roles*]].

Supplemental Guidance: This control enhancement is applied in addition to the monitoring for unauthorized remote connections and mobile devices. Monitoring for unauthorized system components may be accomplished on an ongoing basis or by the periodic scanning of systems for that purpose. Automated mechanisms can be implemented within information systems or in other separate devices. Isolation can be achieved, for example, by placing unauthorized information system components in separate domains or subnets or otherwise quarantining such components. This type of component isolation is commonly referred to as sandboxing. Related controls: AC-17, AC-18, AC-19, CA-7, SI-3, SI-4, SI-7, RA-5.

(4) *INFORMATION SYSTEM COMPONENT INVENTORY | ACCOUNTABILITY INFORMATION*

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

Supplemental Guidance: Identifying individuals who are both responsible and accountable for administering information system components helps to ensure that the assigned components are properly administered and organizations can contact those individuals if some action is required (e.g., component is determined to be the source of a breach/compromise, component needs to be recalled/replaced, or component needs to be relocated).

(5) *INFORMATION SYSTEM COMPONENT INVENTORY | NO DUPLICATE ACCOUNTING OF COMPONENTS*

The organization verifies that all components within the authorization boundary of the information system are not duplicated in other information system inventories.

Supplemental Guidance: This control enhancement addresses the potential problem of duplicate accounting of information system components in large or complex interconnected systems.

(6) *INFORMATION SYSTEM COMPONENT INVENTORY | ASSESSED CONFIGURATIONS / APPROVED DEVIATIONS*

The organization includes assessed component configurations and any approved deviations to current deployed configurations in the information system component inventory.

Supplemental Guidance: This control enhancement focuses on configuration settings established by organizations for information system components, the specific components that have been assessed to determine compliance with the required configuration settings, and any approved deviations from established configuration settings. Related controls: CM-2, CM-6.

(7) *INFORMATION SYSTEM COMPONENT INVENTORY | CENTRALIZED REPOSITORY*

The organization provides a centralized repository for the inventory of information system components.

Supplemental Guidance: Organizations may choose to implement centralized information system component inventories that include components from all organizational information systems. Centralized repositories of information 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 (e.g., information system association, information system owner).

(8) *INFORMATION SYSTEM COMPONENT INVENTORY | AUTOMATED LOCATION TRACKING*

The organization employs automated mechanisms to support tracking of information system components by geographic location.

Supplemental Guidance: The use of automated mechanisms to track the location of information system components can increase the accuracy of component inventories. Such capability may also help organizations rapidly identify the location and responsible individuals of system

Deleted: addition

Deleted: /devices into

Deleted: Disables

Deleted: /devices or

Deleted: designated organizational officials.

Deleted: Enhancement

Deleted: in AC-17 and for unauthorized

Deleted: in AC-19. The monitoring

Deleted: components/devices on information

Deleted: networks

Deleted: organizational networks

Deleted:

Deleted: the

Deleted: and/or in another separate information system or device.

Deleted: 19

Deleted: property accountability information for

Deleted: components

Deleted:]

Deleted: either inventoried as a part of the system or recognized by another system as a component within that system

Deleted: Enhancement

Deleted: the

Deleted: the organization

Deleted: its

Deleted: information system

Deleted: in the deployed information system components

components that have been compromised, breached, or are otherwise in need of mitigation actions.

(9) *INFORMATION SYSTEM COMPONENT INVENTORY | ASSIGNMENT OF COMPONENTS TO SYSTEMS*

The organization:

(a) Assigns [*Assignment: organization-defined acquired information system components*] to an information system; and

(b) Receives an acknowledgement from the information system owner of this assignment.

Supplemental Guidance: Organizations determine the criteria for or types of information system components (e.g., microprocessors, motherboards, software, programmable logic controllers, and network devices) that are subject to this control enhancement. Related control: SA-4.

References: NIST Special Publication 800-128.

Priority and Baseline Allocation:

P1	**LOW** CM-8	**MOD** CM-8 (1) (3) (5)	**HIGH** CM-8 (1) (2) (3) (4) (5)

CM-9 CONFIGURATION MANAGEMENT PLAN

Control: The organization develops, documents, and implements a configuration management plan for the information system that:

a. Addresses roles, responsibilities, and configuration management processes and procedures;

b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;

c. Defines the configuration items for the information system and places the configuration items under configuration management; and

d. Protects the configuration management plan from unauthorized disclosure and modification.

Supplemental Guidance: Configuration management plans satisfy the requirements in configuration management policies while being tailored to individual information systems. Such plans define detailed processes and procedures for how configuration management is used to support system development life cycle activities at the information system level. Configuration management plans are typically developed during the development/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 information system component inventories, how to control development, test, and operational environments, and how to develop, release, and update key documents. Organizations can employ templates to help ensure consistent and timely development and implementation of configuration management plans. Such templates can represent a master configuration management plan for the organization at large with subsets of the plan implemented on a system by system basis. Configuration management approval processes include designation of key management stakeholders responsible for reviewing and approving proposed changes to information systems, and personnel that conduct security impact analyses prior to the implementation of changes to the systems. Configuration items are the information system items (hardware, software, firmware, and documentation) to be configuration-managed. As information systems continue through the system development life cycle, new configuration items may be identified and some existing configuration items may no longer need to be under configuration control. Related controls: CM-2, CM-3, CM-4, CM-5, CM-8, SA-10.

Control Enhancements:

(1) *CONFIGURATION MANAGEMENT PLAN | ASSIGNMENT OF RESPONSIBILITY*

The organization assigns responsibility for developing the configuration management process to organizational personnel that are not directly involved in information system development.

Deleted: <#>Defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management; and¶

Deleted: the means

Deleted: a process

Deleted: items are the information system items (hardware, software, firmware, and documentation) to be configuration managed. The

Deleted: plan satisfies the requirements in the organization's configuration management policy

Deleted: the

Deleted: system. The configuration management plan defines

Deleted: The plan describes how to move a change through the change

Deleted: process, how

Deleted: configuration

Deleted: are updated

Deleted: the

Deleted: inventory is maintained

Deleted: are controlled

Deleted: finally,

Deleted: are developed, released, and updated. The configuration

Deleted: process includes

Deleted: that are

Deleted: the

Deleted: system

Deleted: security

Deleted: would

Deleted: an

Deleted: analysis

Deleted: any changes to

Deleted: .

Deleted: control:

Supplemental Guidance: In the absence of dedicated configuration management teams assigned within organizations, system developers may be tasked to develop configuration management processes using personnel who are not directly involved in system development or integration. This separation of duties ensures that organizations establish and maintain a sufficient degree of independence between the information system development and integration processes and configuration management processes to facilitate quality control and more effective oversight.

Deleted: Enhancement

Deleted: a

Deleted: team, the

Deleted: integrator

Deleted: with developing the configuration management process

References: NIST Special Publication 800-128.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** CM-9	**HIGH** CM-9

CM-10 SOFTWARE USAGE RESTRICTIONS

Control: The organization:

Deleted: develops, disseminates,

a. Uses software and associated documentation in accordance with contract agreements and copyright laws;

b. Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and

Moved (insertion) [6]

c. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

Supplemental Guidance: Software license tracking can be accomplished by manual methods (e.g., simple spreadsheets) or automated methods (e.g., specialized tracking applications) depending on organizational needs. Related controls: AC-17, CM-8, SC-7.

Control Enhancements:

(1) *SOFTWARE USAGE RESTRICTIONS | OPEN SOURCE SOFTWARE*

The organization establishes the following restrictions on the use of open source software: [*Assignment: organization-defined restrictions*].

Supplemental Guidance: Open source software refers to software that is available in source code form. Certain software rights normally reserved for copyright holders are routinely provided under software license agreements that permit individuals to study, change, and improve the software. From a security perspective, the major advantage of open source software is that it provides organizations with the ability to examine the source code. However, there are also various licensing issues associated with open source software including, for example, the constraints on derivative use of such software.

References: None.

Priority and Baseline Allocation:

P2	**LOW** CM-10	**MOD** CM-10	**HIGH** CM-10

CM-11 USER-INSTALLED SOFTWARE

Control: The organization:

a. Establishes [*Assignment: organization-defined policies*] governing the installation of software by users;

b. Enforces software installation policies through [*Assignment: organization-defined methods*]; and

c. Monitors policy compliance at [*Assignment: organization-defined frequency*].

Supplemental Guidance: If provided the necessary privileges, users have the ability to install software in organizational information systems. To maintain control over the types of software installed, organizations identify permitted and prohibited actions regarding software installation. Permitted software installations may include, for example, updates and security patches to existing software and downloading applications from organization-approved “app stores.” Prohibited software installations may include, for example, software with unknown or suspect pedigrees or software that organizations consider potentially malicious. The policies organizations select governing user-installed software may be organization-developed or provided by some external entity. Policy enforcement methods include procedural methods (e.g., periodic examination of user accounts), automated methods (e.g., configuration settings implemented on organizational information systems), or both. Related controls: AC-3, CM-2, CM-3, CM-5, CM-6, CM-7, PL-4.

Control Enhancements:

(1) *USER-INSTALLED SOFTWARE | ALERTS FOR UNAUTHORIZED INSTALLATIONS*

The information system alerts [*Assignment: organization-defined personnel or roles*] when the unauthorized installation of software is detected.

Supplemental Guidance: Related controls: CA-7, SI-4.

(2) *USER-INSTALLED SOFTWARE | PROHIBIT INSTALLATION WITHOUT PRIVILEGED STATUS*

The information system prohibits user installation of software without explicit privileged status.

Supplemental Guidance: Privileged status can be obtained, for example, by serving in the role of system administrator. Related control: AC-6.

References: None.

Moved (insertion) [7]

Priority and Baseline Allocation:

P1	**LOW** CM-11	**MOD** CM-11	**HIGH** CM-11

FAMILY: CONTINGENCY PLANNING

CP-1 CONTINGENCY PLANNING POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

1. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls; and

Deleted: Formal, documented procedures

Deleted: .

b. Reviews and updates the current:

1. Contingency planning policy [*Assignment: organization-defined frequency*]; and

2. Contingency planning procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the CP family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Deleted: is intended to produce

Deleted: that are required

Deleted: contingency planning

Deleted: The policy

Deleted: are consistent with

Deleted: policies,

Deleted: Existing organizational

Deleted: additional

Deleted:

Deleted: contingency planning

Deleted: the organization. Contingency planning

Deleted: developed

Deleted: a

Deleted: system, when required.

Deleted: the development of the contingency planning

Deleted: .

Control Enhancements: None.

References: Federal Continuity Directive 1; NIST Special Publications 800-12, 800-34, 800-100.

Priority and Baseline Allocation:

P1	**LOW** CP-1	**MOD** CP-1	**HIGH** CP-1

CP-2 CONTINGENCY PLAN

Control: The organization:

a. Develops a contingency plan for the information system that:

1. Identifies essential missions and business functions and associated contingency requirements;

2. Provides recovery objectives, restoration priorities, and metrics;

3. Addresses contingency roles, responsibilities, assigned individuals with contact information;

4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;

5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and

6. Is reviewed and approved by [*Assignment: organization-defined personnel or roles*];

Deleted: measures

Deleted: designated officials within the

Deleted: ;

b. Distributes copies of the contingency plan to [*Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements*];

c. Coordinates contingency planning activities with incident handling activities;

d. Reviews the contingency plan for the information system [*Assignment: organization-defined frequency*];

e. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;

f. Communicates contingency plan changes to [*Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements*]; and

g. Protects the contingency plan from unauthorized disclosure and modification.

Supplemental Guidance: Contingency planning for information systems is part of an overall organizational program for achieving continuity of operations for mission/business functions. Contingency planning addresses both information system restoration and implementation of alternative mission/business processes when systems are compromised. The effectiveness of contingency planning is maximized by considering such planning throughout the phases of the system development life cycle. Performing contingency planning on hardware, software, and firmware development can be an effective means of achieving information system resiliency. Contingency plans reflect the degree of restoration required for organizational information systems since not all systems may need to fully recover to achieve the level of continuity of operations desired. Information system recovery objectives reflect applicable laws, Executive Orders, directives, policies, standards, regulations, and guidelines. In addition to information system availability, contingency plans also address other security-related events resulting in a reduction in mission and/or business effectiveness, such as malicious attacks compromising the confidentiality or integrity of information systems. Actions addressed in contingency plans include, for example, orderly/graceful degradation, information system shutdown, fallback to a manual mode, alternate information flows, and operating in modes reserved for when systems are under attack. By closely coordinating contingency planning with incident handling activities, organizations can ensure that the necessary contingency planning activities are in place and activated in the event of a security incident. Related controls: AC-14, CP-6, CP-7, CP-8, CP-9, CP-10, IR-4, IR-8, MP-2, MP-4, MP-5, PM-8, PM-11.

Control Enhancements:

(1) *CONTINGENCY PLAN | COORDINATE WITH RELATED PLANS*

The organization coordinates contingency plan development with organizational elements responsible for related plans.

Supplemental Guidance: Plans related to contingency plans for organizational information 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.

(2) *CONTINGENCY PLAN | CAPACITY PLANNING*

The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.

Supplemental Guidance: Capacity planning is needed because different types of threats (e.g., natural disasters, targeted cyber attacks) can result in a reduction of the available processing, telecommunications, and support services originally intended to support the organizational missions/business functions. Organizations may need to anticipate degraded operations during contingency operations and factor such degradation into capacity planning.

(3) *CONTINGENCY PLAN | RESUME ESSENTIAL MISSIONS / BUSINESS FUNCTIONS*

The organization plans for the resumption of essential missions and business functions within [*Assignment: organization-defined time period*] of contingency plan activation.

Deleted: *list of*

Deleted: Revises

Deleted: and

Deleted: *list of*

Deleted:].

Deleted: operations.

Deleted: are consistent with

Deleted: or

Deleted: .

Deleted: /

Deleted: the

Deleted: system. Examples of actions to call out

Deleted: fall back

Deleted: or

Deleted: a mode that is

Deleted: solely

Deleted: the system is

Deleted: Enhancement

Deleted: Examples of

Deleted: Plan

Deleted: Plan

Deleted: Plan

Deleted: Plan

Deleted: Plan

Deleted: Plan

Supplemental Guidance: Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. The time period for resumption of essential missions/business functions may be dependent on the severity/extent of disruptions to the information system and its supporting infrastructure. Related control: PE-12.

(4) *CONTINGENCY PLAN | RESUME ALL MISSIONS / BUSINESS FUNCTIONS*

The organization plans for the resumption of all missions and business functions within [*Assignment: organization-defined time period*] of contingency plan activation.

Deleted: full

Supplemental Guidance: Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. The time period for resumption of all missions/business functions may be dependent on the severity/extent of disruptions to the information system and its supporting infrastructure. Related control: PE-12.

(5) *CONTINGENCY PLAN | CONTINUE ESSENTIAL MISSIONS / BUSINESS FUNCTIONS*

The organization plans for the continuance of essential missions and business functions with little or no loss of operational continuity and sustains that continuity until full information system restoration at primary processing and/or storage sites.

Supplemental Guidance: Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. Primary processing and/or storage sites defined by organizations as part of contingency planning may change depending on the circumstances associated with the contingency (e.g., backup sites may become primary sites). Related control: PE-12.

(6) *CONTINGENCY PLAN | ALTERNATE PROCESSING / STORAGE SITE*

The organization plans 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 sustains that continuity through information system restoration to primary processing and/or storage sites.

Deleted: provides

Deleted: all

Supplemental Guidance: Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. Primary processing and/or storage sites defined by organizations as part of contingency planning may change depending on the circumstances associated with the contingency (e.g., backup sites may become primary sites). Related control: PE-12.

(7) *CONTINGENCY PLAN | COORDINATE WITH EXTERNAL SERVICE PROVIDERS*

The organization coordinates its contingency plan with the contingency plans of external service providers to ensure that contingency requirements can be satisfied.

Supplemental Guidance: When the capability of an organization to successfully carry out its core missions/business functions is dependent on external service providers, developing a timely and comprehensive contingency plan may become more challenging. In this situation, organizations coordinate contingency planning activities with the external entities to ensure that the individual plans reflect the overall contingency needs of the organization. Related control: SA-9.

(8) *CONTINGENCY PLAN | IDENTIFY CRITICAL ASSETS*

The organization identifies critical information system assets supporting essential missions and business functions.

Supplemental Guidance: Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. Organizations identify critical information system assets so that additional safeguards and countermeasures can be employed (above and beyond those safeguards and countermeasures routinely implemented) to help ensure that organizational missions/business functions can continue to be conducted during contingency operations. In addition, the identification of critical information assets facilitates the prioritization of organizational resources. Critical information system assets include technical and operational aspects. Technical aspects include, for example, information technology services, information 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 provide assistance in identifying critical assets. Related controls: SA-14, SA-15.

References: Federal Continuity Directive 1; NIST Special Publication 800-34.

Priority and Baseline Allocation:

P1	**LOW** CP-2	**MOD** CP-2 (1) (3) (8)	**HIGH** CP-2 (1) (2) (3) (4) (5) (8)

CP-3 CONTINGENCY TRAINING

Control: The organization provides contingency training to information system users consistent with assigned roles and responsibilities:

a. Within [*Assignment: organization-defined time period*] of assuming a contingency role or responsibility;

b. When required by information system changes; and

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

Supplemental Guidance: Contingency training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail is included in such training. For example, regular users may only need to know when and where to report for duty during contingency operations and if normal duties are affected; system administrators may require additional training on how to set up information systems at alternate processing and storage sites; and managers/senior leaders may receive more specific training on how to conduct mission-essential functions in designated off-site locations and how to establish communications with other governmental entities for purposes of coordination on contingency-related activities. Training for contingency roles/responsibilities reflects the specific continuity requirements in the contingency plan. Related controls: AT-2, AT-3, CP-2, IR-2.

Control Enhancements:

(1) *CONTINGENCY TRAINING | SIMULATED EVENTS*

The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.

(2) *CONTINGENCY TRAINING | AUTOMATED TRAINING ENVIRONMENTS*

The organization employs automated mechanisms to provide a more thorough and realistic contingency training environment.

References: Federal Continuity Directive 1; NIST Special Publications 800-16, 800-50.

Priority and Baseline Allocation:

P2	**LOW** CP-3	**MOD** CP-3	**HIGH** CP-3 (1)

CP-4 CONTINGENCY PLAN TESTING

Control: The organization:

a. Tests the contingency plan for the information system [*Assignment: organization-defined frequency*] using [*Assignment: organization-defined tests*] to determine the effectiveness of the plan and the organizational readiness to execute the plan;

b. Reviews the contingency plan test results; and

Deleted: trains personnel in their

Deleted: with respect to the

Deleted: provides refresher training

Deleted: None.

Deleted: AND EXERCISES

Deleted: and/or exercises

Deleted: *and/or exercises*

Deleted: plan's

Deleted: organization's

Deleted: and

Deleted: /exercise

Deleted: initiates

c. Initiates corrective actions, if needed.

Supplemental Guidance: Methods for testing contingency plans to determine the effectiveness of the plans and to identify potential weaknesses in the plans include, for example, walk-through and tabletop exercises, checklists, simulations (parallel, full interrupt), and comprehensive exercises. Organizations conduct testing based on the continuity requirements in contingency plans and include a determination of the effects on organizational operations, assets, and individuals arising due to contingency operations. Organizations have flexibility and discretion in the breadth, depth, and timelines of corrective actions. Related controls: CP-2, CP-3, IR-3.

Control Enhancements:

(1) *CONTINGENCY PLAN TESTING | COORDINATE WITH RELATED PLANS*

The organization coordinates contingency plan testing with organizational elements responsible for related plans.

Supplemental Guidance: Plans related to contingency plans for organizational information systems include, for example, Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, and Occupant Emergency Plans. This control enhancement does not require organizations to create organizational elements to handle related plans or to align such elements with specific plans. It does require, however, that if such organizational elements are responsible for related plans, organizations should coordinate with those elements. Related controls: IR-8, PM-8.

(2) *CONTINGENCY PLAN TESTING | ALTERNATE PROCESSING SITE*

The organization tests the contingency plan at the alternate processing site:

(a) To familiarize contingency personnel with the facility and available resources; and

(b) To evaluate the capabilities of the alternate processing site to support contingency operations.

Supplemental Guidance: Related control: CP-7.

(3) *CONTINGENCY PLAN TESTING | AUTOMATED TESTING*

The organization employs automated mechanisms to more thoroughly and effectively test the contingency plan.

Supplemental Guidance: Automated mechanisms provide more thorough and effective testing of contingency plans, for example: (i) by providing more complete coverage of contingency issues; (ii) by selecting more realistic test scenarios and environments; and (iii) by effectively stressing the information system and supported missions.

(4) *CONTINGENCY PLAN TESTING | FULL RECOVERY / RECONSTITUTION*

The organization includes a full recovery and reconstitution of the information system to a known state as part of contingency plan testing.

Supplemental Guidance: Related controls: CP-10, SC-24.

References: Federal Continuity Directive 1; FIPS Publication 199; NIST Special Publications 800-34, 800-84.

P2	LOW CP-4	MOD CP-4 (1)	HIGH CP-4 (1) (2)

CP-5 CONTINGENCY PLAN UPDATE

[Withdrawn: Incorporated into CP-2].

CP-6 ALTERNATE STORAGE SITE

Control: The organization:

Deleted: There are several methods

Deleted: and/or exercising

Deleted: (e.g., checklist

Deleted: /

Deleted: , simulation:

Deleted:). Contingency plan

Deleted: and/or exercises

Deleted: and

Deleted: (e.g., reduction in mission capability)

Deleted: and/or exercises

Deleted: Enhancement

Deleted: Examples of

Deleted: Plan

Deleted: Plan

Deleted: Plan

Deleted: Plan

Deleted: Plan

Deleted: Plan

Deleted: Plan

Deleted: /exercises

Deleted: site's

Deleted: /exercise

Deleted: by providing more complete coverage of contingency issues, selecting more realistic test/exercise scenarios and environments, and more effectively stressing the information system and supported missions

Deleted: Enhancement

Deleted: (4)

a. Establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information; and

b. Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.

Deleted: recovery

Deleted: .

Supplemental Guidance: Alternate storage sites are sites that are geographically distinct from primary storage sites. An alternate storage site maintains duplicate copies of information and data in the event that 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/business functions despite disruption, compromise, or failure in organizational information systems. Related controls: CP-2, CP-7, CP-9, CP-10, MP-4.

Control Enhancements:

(1) *ALTERNATE STORAGE SITE | SEPARATION FROM PRIMARY SITE*

The organization identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.

Supplemental Guidance: Threats that affect alternate storage sites are typically defined in organizational assessments of risk and include, for example, natural disasters, structural failures, hostile cyber attacks, and errors of omission/commission. Organizations determine what is considered a sufficient degree of separation between primary and alternate storage sites based on the types of threats that are of concern. For one particular type of threat (i.e., hostile cyber attack), the degree of separation between sites is less relevant. Related control: RA-3.

Deleted: so as not

Deleted: be susceptible

Deleted: hazards

Deleted: Enhancement Supplemental Guidance: Hazards of concern to the organization are typically defined in an organizational assessment of risk.¶

(2) *ALTERNATE STORAGE SITE | RECOVERY TIME / POINT OBJECTIVES*

The organization configures the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.

(3) *ALTERNATE STORAGE SITE | ACCESSIBILITY*

The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

Supplemental Guidance: Area-wide disruptions refer to those types of disruptions that are broad in geographic scope (e.g., hurricane, regional power outage) with such determinations made by organizations based on organizational assessments of risk. Explicit mitigation actions include, for example: (i) duplicating backup information at other alternate storage sites if access problems occur at originally designated alternate sites; or (ii) planning for physical access to retrieve backup information if electronic accessibility to the alternate site is disrupted. Related control: RA-3.

Deleted: Enhancement

Deleted: ,

Deleted: another

Deleted: site

Deleted: to the first

Deleted: site is hindered

Deleted: ,

Deleted: , planning for physical access to retrieve backup information

References: NIST Special Publication 800-34.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** CP-6 (1) (3)	**HIGH** CP-6 (1) (2) (3)

CP-7 ALTERNATE PROCESSING SITE

Control: The organization:

a. Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of [*Assignment: organization-defined information system operations*] for essential missions/business functions within [*Assignment: organization-defined time period consistent with recovery time and recovery point objectives*] when the primary processing capabilities are unavailable;

Deleted: and

Deleted: and

b. Ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and

Deleted: in time to support

Deleted: .

c. Ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site.

Supplemental Guidance: Alternate processing sites are sites that are geographically distinct from primary processing sites. An alternate processing site provides processing capability in the event that the primary processing site is not available. Items covered by alternate processing site agreements include, for example, environmental conditions at alternate sites, access rules, physical and environmental protection requirements, and coordination for the transfer/assignment of personnel. Requirements are specifically allocated to alternate processing sites that reflect the requirements in contingency plans to maintain essential missions/business functions despite disruption, compromise, or failure in organizational information systems. Related controls: CP-2, CP-6, CP-8, CP-9, CP-10, MA-6.

Control Enhancements:

(1) *ALTERNATE PROCESSING SITE | SEPARATION FROM PRIMARY SITE*

The organization identifies an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.

Supplemental Guidance: Threats that affect alternate processing sites are typically defined in organizational assessments of risk and include, for example, natural disasters, structural failures, hostile cyber attacks, and errors of omission/commission. Organizations determine what is considered a sufficient degree of separation between primary and alternate processing sites based on the types of threats that are of concern. For one particular type of threat (i.e., hostile cyber attack), the degree of separation between sites is less relevant. Related control: RA-3.

Deleted: so as not

Deleted: be susceptible

Deleted: hazards

Deleted: Enhancement Supplemental Guidance: Hazards that might affect the information system are typically defined in the risk assessment.¶

(2) *ALTERNATE PROCESSING SITE | ACCESSIBILITY*

The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

Supplemental Guidance: Area-wide disruptions refer to those types of disruptions that are broad in geographic scope (e.g., hurricane, regional power outage) with such determinations made by organizations based on organizational assessments of risk. Related control: RA-3.

(3) *ALTERNATE PROCESSING SITE | PRIORITY OF SERVICE*

The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives).

Deleted: the organization's

Deleted: .

Supplemental Guidance: Priority-of-service agreements refer to negotiated agreements with service providers that ensure that organizations receive priority treatment consistent with their availability requirements and the availability of information resources at the alternate processing site.

(4) *ALTERNATE PROCESSING SITE | PREPARATION FOR USE*

The organization prepares the alternate processing site so that the site is ready to be used as the operational site supporting essential missions and business functions.

Deleted: configures

Deleted: it

Supplemental Guidance: Site preparation includes, for example, establishing configuration settings for information system components at the alternate processing site consistent with the requirements for such settings at the primary site and ensuring that essential supplies and other logistical considerations are in place. Related controls: CM-2, CM-6.

(5) *ALTERNATE PROCESSING SITE | EQUIVALENT INFORMATION SECURITY SAFEGUARDS*

[Withdrawn: Incorporated into CP-7].

Deleted: The organization ensures that the alternate processing site provides information security measures equivalent to that of the primary site.

(6) *ALTERNATE PROCESSING SITE | INABILITY TO RETURN TO PRIMARY SITE*

The organization plans and prepares for circumstances that preclude returning to the primary processing site.

References: NIST Special Publication 800-34.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** CP-7 (1) (2) (3)	**HIGH** CP-7 (1) (2) (3) (4)

Deleted: (5)

Deleted: (5)

CP-8 TELECOMMUNICATIONS SERVICES

Control: The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of [*Assignment: organization-defined information system operations*] for essential missions and business functions within [*Assignment: organization-defined time period*] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

Supplemental Guidance: This control applies to telecommunications services (data and voice) for primary and alternate processing and storage sites. Alternate telecommunications services reflect the continuity requirements in contingency plans to maintain essential missions/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 into alternate telecommunications agreements. Related controls: CP-2, CP-6, CP-7.

Control Enhancements:

(1) *TELECOMMUNICATIONS SERVICES | PRIORITY OF SERVICE PROVISIONS*

The organization:

(a) Develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives); and

Deleted: the organization's

Deleted: ;

(b) Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.

Supplemental Guidance: Organizations consider the potential mission/business impact in situations where telecommunications service providers are servicing other organizations with similar priority-of-service provisions.

(2) *TELECOMMUNICATIONS SERVICES | SINGLE POINTS OF FAILURE*

The organization obtains alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

Deleted: with consideration for reducing

(3) *TELECOMMUNICATIONS SERVICES | SEPARATION OF PRIMARY / ALTERNATE PROVIDERS*

The organization obtains alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.

Deleted: service

Deleted: so as not to be susceptible

Deleted: hazards

Supplemental Guidance: Threats that affect telecommunications services are typically defined in organizational assessments of risk and include, for example, natural disasters, structural failures, hostile cyber/physical attacks, and errors of omission/commission. Organizations seek to reduce common susceptibilities by, for example, minimizing shared infrastructure among telecommunications service providers and achieving sufficient geographic separation between services. Organizations may consider using a single service provider in situations where the service provider can provide alternate telecommunications services meeting the separation needs addressed in the risk assessment.

(4) *TELECOMMUNICATIONS SERVICES | PROVIDER CONTINGENCY PLAN*

The organization:

(a) Requires primary and alternate telecommunications service providers to have contingency plans;

(b) Reviews provider contingency plans to ensure that the plans meet organizational contingency requirements; and

(c) Obtains evidence of contingency testing/training by providers [*Assignment: organization-defined frequency*].

Supplemental Guidance: Reviews of provider contingency plans consider the proprietary nature of such plans. In some situations, a summary of provider contingency plans may be sufficient evidence for organizations to satisfy the review requirement. Telecommunications service providers may also participate in ongoing disaster recovery exercises in coordination with the Department of Homeland Security, state, and local governments. Organizations may use these types of activities to satisfy evidentiary requirements related to service provider contingency plan reviews, testing, and training.

(5) *TELECOMMUNICATIONS SERVICES | ALTERNATE TELECOMMUNICATION SERVICE TESTING*

The organization tests alternate telecommunication services [*Assignment: organization-defined frequency*].

References: NIST Special Publication 800-34; National Communications Systems Directive 3-10; Web: tsp.ncs.gov.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** CP-8 (1) (2)	**HIGH** CP-8 (1) (2) (3) (4)

CP-9 INFORMATION SYSTEM BACKUP

Control: The organization:

a. Conducts backups of user-level information contained in the information system [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*];

b. Conducts backups of system-level information contained in the information system [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*];

c. Conducts backups of information system documentation including security-related documentation [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*]; and

d. Protects the confidentiality, integrity, and availability of backup information at storage locations.

Deleted: and

Deleted: the

Supplemental Guidance: System-level information includes, for example, system-state information, operating system and application software, and licenses. User-level information includes any information other than system-level information. Mechanisms employed by organizations to protect the integrity of information system backups include, for example, digital signatures and cryptographic hashes. Protection of system backup information while in transit is beyond the scope of this control. Information system backups reflect the requirements in contingency plans as well as other organizational requirements for backing up information. Related controls: CP-2, CP-6, MP-4, MP-5, SC-13.

Deleted: Digital signatures and cryptographic hashes are examples of mechanisms that can be

Deleted: . An organizational assessment of risk guides the use of encryption

Deleted: protecting backup information. The protection

Control Enhancements:

(1) *INFORMATION SYSTEM BACKUP | TESTING FOR RELIABILITY / INTEGRITY*

The organization tests backup information [*Assignment: organization-defined frequency*] to verify media reliability and information integrity.

Supplemental Guidance: Related control: CP-4.

(2) *INFORMATION SYSTEM BACKUP | TEST RESTORATION USING SAMPLING*

The organization uses a sample of backup information in the restoration of selected information system functions as part of contingency plan testing.

Supplemental Guidance: Related control: CP-4.

(3) *INFORMATION SYSTEM BACKUP | SEPARATE STORAGE FOR CRITICAL INFORMATION*

The organization stores backup copies of [*Assignment: organization-defined critical information system software and other security-related information*] in a separate facility or in a fire-rated container that is not collocated with the operational system.

Supplemental Guidance: Critical information system software includes, for example, operating systems, cryptographic key management systems, and intrusion detection/prevention systems. Security-related information includes, for example, organizational inventories of hardware, software, and firmware components. Alternate storage sites typically serve as separate storage facilities for organizations. Related controls: CM-2, CM-8.

(4) *INFORMATION SYSTEM BACKUP | PROTECTION FROM UNAUTHORIZED MODIFICATION*

[Withdrawn: Incorporated into CP-9].

(5) *INFORMATION SYSTEM BACKUP | TRANSFER TO ALTERNATE STORAGE SITE*

The organization transfers information system backup information to the alternate storage site [*Assignment: organization-defined time period and transfer rate consistent with the recovery time and recovery point objectives*].

Supplemental Guidance: Information system backup information can be transferred to alternate storage sites either electronically or by physical shipment of storage media.

(6) *INFORMATION SYSTEM BACKUP | REDUNDANT SECONDARY SYSTEM*

The organization accomplishes information system backup by maintaining a redundant secondary system that is not collocated with the primary system and that can be activated without loss of information or disruption to operations.

Supplemental Guidance: Related controls: CP-7, CP-10.

(7) *INFORMATION SYSTEM BACKUP | DUAL AUTHORIZATION*

The organization enforces dual authorization for the deletion or destruction of [*Assignment: organization-defined backup information*].

Supplemental Guidance: Dual authorization ensures that the deletion or destruction of backup information cannot occur unless two qualified individuals carry out the task. Individuals deleting/destroying backup information possess sufficient skills/expertise to determine if the proposed deletion/destruction of backup information reflects organizational policies and procedures. Related controls: AC-3, MP-2.

References: NIST Special Publication 800-34.

Priority and Baseline Allocation:

P1	**LOW** CP-9	**MOD** CP-9 (1)	**HIGH** CP-9 (1) (2) (3) (5)

CP-10 INFORMATION SYSTEM RECOVERY AND RECONSTITUTION

Control: The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.

Supplemental Guidance: Recovery is executing information system contingency plan activities to restore organizational missions/business functions. Reconstitution takes place following recovery and includes activities for returning organizational information 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 information system capabilities that may have been needed during recovery operations. Reconstitution also includes assessments of fully restored information system capabilities, reestablishment of continuous monitoring activities, potential information system reauthorizations, and activities to prepare the systems against future disruptions, compromises, or failures. Recovery/reconstitution capabilities

Deleted: the operating system and other

Deleted: , as well as copies of the information system inventory (including hardware, software, and firmware components)

Deleted: colocated

Deleted: ,

Deleted: ,

Deleted: the operation

Deleted: essential

Deleted: and

Deleted:

Deleted: the

Deleted: system

Deleted: its original functional state before contingency plan activation.

Deleted: procedures are based on organizational

Deleted: established

Deleted: appropriate

Deleted: .

Deleted: capability

Deleted:

Deleted: an assessment

Deleted: the

Deleted: capability, a

Deleted: reauthorization

Deleted: the necessary

Deleted: system

Deleted: another disruption, compromise

Deleted: failure.

Deleted: and

employed by organizations can include both automated mechanisms and manual procedures. Related controls: CA-2, CA-6, CA-7, CP-2, CP-6, CP-7, CP-9, SC-24.

Control Enhancements:

(1) *INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | CONTINGENCY PLAN TESTING*

[Withdrawn: Incorporated into CP-4].

(2) *INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | TRANSACTION RECOVERY*

The information system implements transaction recovery for systems that are transaction-based.

Supplemental Guidance: Transaction-based information systems include, for example, database management systems and transaction processing systems. Mechanisms supporting transaction recovery include, for example, transaction rollback and transaction journaling.

(3) *INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | COMPENSATING SECURITY CONTROLS*

[Withdrawn: Addressed through tailoring procedures].

(4) *INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | RESTORE WITHIN TIME PERIOD*

The organization provides the capability to restore information system components within [*Assignment: organization-defined restoration time-periods*] from configuration-controlled and integrity-protected information representing a known, operational state for the components.

Supplemental Guidance: Restoration of information system components includes, for example, reimaging which restores components to known, operational states. Related control: CM-2.

(5) *INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | FAILOVER CAPABILITY*

[Withdrawn: Incorporated into SI-13].

(6) *INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | COMPONENT PROTECTION*

The organization protects backup and restoration hardware, firmware, and software.

Supplemental Guidance: Protection of backup and restoration hardware, firmware, and software components includes both physical and technical safeguards. Backup and restoration software includes, for example, router tables, compilers, and other security-relevant system software. Related controls: AC-3, AC-6, PE-3.

References: Federal Continuity Directive 1; NIST Special Publication 800-34.

Priority and Baseline Allocation:

P1	**LOW** CP-10	**MOD** CP-10 (2)	**HIGH** CP-10 (2) (4)

CP-11 ALTERNATE COMMUNICATIONS PROTOCOLS

Control: The information system provides the capability to employ [*Assignment: organization-defined alternative communications protocols*] in support of maintaining continuity of operations.

Supplemental Guidance: Contingency plans and the associated training and testing for those plans, incorporate an alternate communications protocol capability as part of increasing the resilience of organizational information systems. Alternate communications protocols include, for example, switching from Transmission Control Protocol/Internet Protocol (TCP/IP) Version 4 to TCP/IP Version 6. Switching communications protocols may affect software applications and therefore, the potential side effects of introducing alternate communications protocols are analyzed prior to implementation.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

Deleted: the organization

Deleted: be a combination of

Deleted:

Deleted: Enhancement

Deleted: Database

Deleted: are examples of information systems that are

Deleted: -based. Transaction

Deleted: are examples of mechanisms supporting transaction recovery

Deleted: The organization provides compensating security controls for [*Assignment: organization-defined circumstances that can inhibit recovery and reconstitution to a known state*].¶

Deleted: reimage

Deleted: disk images

Deleted: secure

Deleted: The organization provides [*Selection: real-time; near-real-time*] [*Assignment: organization-defined failover capability for the information system*].¶
Enhancement Supplemental Guidance: Examples of failover capability are incorporating mirrored information system operations at an alternate processing site or periodic data mirroring at regular intervals during a time period defined by the organization's recovery time period.¶

Deleted: Enhancement

Deleted: measures. Router

Deleted: are examples of backup and restoration software

Deleted: (3)

Deleted: (3)

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

CP-12 SAFE MODE

Control: The information system, when [*Assignment: organization-defined conditions*] are detected, enters a safe mode of operation with [*Assignment: organization-defined restrictions of safe mode of operation*].

Supplemental Guidance: For information systems supporting critical missions/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 may choose to 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 types of activities or operations information systems could execute when those conditions are encountered. Restriction includes, for example, allowing only certain functions that could be carried out under limited power or with reduced communications bandwidth.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

CP-13 ALTERNATIVE SECURITY MECHANISMS

Control: The organization employs [*Assignment: organization-defined alternative or supplemental security mechanisms*] for satisfying [*Assignment: organization-defined security functions*] when the primary means of implementing the security function is unavailable or compromised.

Supplemental Guidance: This control supports information system resiliency and contingency planning/continuity of operations. To ensure mission/business continuity, organizations can implement alternative or supplemental security mechanisms. These mechanisms may be less effective than the primary mechanisms (e.g., not as easy to use, not as scalable, or not as secure). However, having the capability to readily employ these alternative/supplemental mechanisms enhances overall mission/business continuity that might otherwise be adversely impacted if organizational 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 would typically be applied only to critical security capabilities provided by information systems, system components, or information system services. For example, an organization may issue to senior executives and system administrators one-time pads in case multifactor tokens, the organization's standard means for secure remote authentication, is compromised. Related control: CP-2.

Moved (insertion) [8]

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

FAMILY: IDENTIFICATION AND AUTHENTICATION

IA-1 IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

1. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and

b. Reviews and updates the current:

1. Identification and authentication policy [*Assignment: organization-defined frequency*]; and

2. Identification and authentication procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the IA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: FIPS Publication 201; NIST Special Publications 800-12, 800-63, 800-73, 800-76, 800-78, 800-100.

Priority and Baseline Allocation:

P1	**LOW** IA-1	**MOD** IA-1	**HIGH** IA-1

IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

Control: The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

Supplemental Guidance: Organizational users include employees or individuals that organizations deem to have equivalent status of employees (e.g., contractors, guest researchers). This control applies to all accesses other than: (i) accesses that are explicitly identified and documented in AC-14; and (ii) accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity. Organizations employ passwords, tokens, or biometrics to authenticate user identities, or in the case multifactor authentication, or some combination thereof. Access to organizational information systems is defined as either local access or network access. Local access is any access to organizational information systems by users (or processes acting on behalf of users) where such access is obtained by direct connections without the use of networks. Network access is access to

Deleted:
CLASS: TECHNICAL

Deleted: develops,

Deleted: , and reviews/updates

Deleted: *frequency*

Deleted: A formal, documented

Deleted: Formal, documented procedures

Deleted: .

Deleted: is intended to produce

Deleted: that are required

Deleted: identification and authentication

Deleted: The policy

Deleted: are consistent with

Deleted: policies,

Deleted: Existing organizational

Deleted: additional

Deleted:

Deleted: identification and authentication

Deleted: the organization. Identification and ...

Deleted: developed

Deleted: a

Deleted: system, when required.

Deleted: the development of the identificatio ...

Deleted: .

Deleted: organizational

Deleted: the organization deems

Deleted: , individuals from allied nations). ...

Deleted: those

Deleted: by the organization

Deleted: . Unique

Deleted: may need to be considered

Deleted: Authentication of user identities is ...

Deleted: of

Deleted:

Deleted: .

Deleted: an

Deleted: system

Deleted: a user

Deleted: process

Deleted: a user

Deleted: connection

Deleted: a network.

Deleted: any

organizational information systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks (e.g., the Internet). Internal networks include local area networks and wide area networks. In addition, the use of encrypted virtual private networks (VPNs) for network connections between organization-controlled endpoints and non-organization controlled endpoints may be treated as internal networks from the perspective of protecting the confidentiality and integrity of information traversing the network.

Organizations can satisfy the identification and authentication requirements in this control by complying with the requirements in Homeland Security Presidential Directive 12 consistent with the specific organizational implementation plans. Multifactor authentication requires the use of two or more different factors to achieve authentication. The factors are defined as: (i) something you know (e.g., password, personal identification number [PIN]); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD common access card. In addition to identifying and authenticating users at the information system level (i.e., at logon), organizations also employ identification and authentication mechanisms at the application level, when necessary, to provide increased information security. Identification and authentication requirements for other than organizational users are described in IA-8. Related controls: AC-2, AC-3, AC-14, AC-17, AC-18, IA-4, IA-5, IA-8.

Control Enhancements:

(1) *IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO PRIVILEGED ACCOUNTS*

The information system implements multifactor authentication for network access to privileged accounts.

Supplemental Guidance: Related control: AC-6.

(2) *IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS*

The information system implements multifactor authentication for network access to non-privileged accounts.

(3) *IDENTIFICATION AND AUTHENTICATION | LOCAL ACCESS TO PRIVILEGED ACCOUNTS*

The information system implements multifactor authentication for local access to privileged accounts.

Supplemental Guidance: Related control: AC-6.

(4) *IDENTIFICATION AND AUTHENTICATION | LOCAL ACCESS TO NON-PRIVILEGED ACCOUNTS*

The information system implements multifactor authentication for local access to non-privileged accounts.

(5) *IDENTIFICATION AND AUTHENTICATION | GROUP AUTHENTICATION*

The organization requires individuals to be authenticated with an individual authenticator when a group authenticator is employed.

Supplemental Guidance: Requiring individuals to use individual authenticators as a second level of authentication helps organizations to mitigate the risk of using group authenticators.

(6) *IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO PRIVILEGED ACCOUNTS - SEPARATE DEVICE*

The information system implements multifactor authentication for network access to privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [*Assignment: organization-defined strength of mechanism requirements*].

Supplemental Guidance: Related control: AC-6.

(7) *IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS - SEPARATE DEVICE*

The information system implements multifactor authentication for network access to non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [*Assignment: organization-defined strength of mechanism requirements*].

Deleted: an

Deleted: system

Deleted: a user

Deleted: process

Deleted: a user

Deleted: a

Deleted: connection.

Deleted: which

Deleted: an

Deleted: network

Deleted:

Deleted: ,

Deleted: , and

Deleted: that are under the control of the organization. For a virtual private network (VPN), the VPN is considered an internal network if the organization establishes the VPN connection

Deleted: in a manner that does not require the

Deleted: to depend on any external

Deleted: across which the VPN transits to ...

Deleted: transmitted. Identification and ...

Deleted: The

Deleted: are satisfied

Deleted: organization-

Deleted: provided to OMB.

Deleted: -

Deleted: are employed

Deleted: for the organization.

Deleted: uses

Deleted: uses

Deleted: uses

Deleted: uses

Deleted: ¶ ...

Deleted: prior to

Deleted: a

Deleted: uses

Deleted: where

Deleted: information

Deleted: being accessed.

Deleted: uses

Deleted: where

Deleted: information

Deleted: being accessed.

(8) *IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO PRIVILEGED ACCOUNTS - REPLAY RESISTANT*

The information system implements replay-resistant authentication mechanisms for network access to privileged accounts.

Supplemental Guidance: Authentication processes resist replay attacks if it is impractical to achieve successful authentications by replaying previous authentication messages. Replay-resistant techniques include, for example, protocols that use nonces or challenges such as Transport Layer Security (TLS) and time synchronous or challenge-response one-time authenticators.

(9) *IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS - REPLAY RESISTANT*

The information system implements replay-resistant authentication mechanisms for network access to non-privileged accounts.

Supplemental Guidance: Authentication processes resist replay attacks if it is impractical to achieve successful authentications by recording/replaying previous authentication messages. Replay-resistant techniques include, for example, protocols that use nonces or challenges such as Transport Layer Security (TLS) and time synchronous or challenge-response one-time authenticators.

(10) *IDENTIFICATION AND AUTHENTICATION | SINGLE SIGN-ON*

The information system provides a single sign-on capability for [*Assignment: organization-defined list of information system accounts and services*].

Supplemental Guidance: Single sign-on enables users to log in once and gain access to multiple information system resources. Organizations consider the operational efficiencies provided by single sign-on capabilities with the increased risk from disclosures of single authenticators providing access to multiple system resources.

(11) *IDENTIFICATION AND AUTHENTICATION | REMOTE ACCESS - SEPARATE DEVICE*

The information system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [*Assignment: organization-defined strength of mechanism requirements*].

Supplemental Guidance: For remote access to privileged/non-privileged accounts, the purpose of requiring a device that is separate from the information system gaining access for one of the factors during multifactor authentication is to reduce the likelihood of compromising authentication credentials stored on the system. For example, adversaries deploying malicious code on organizational information systems can potentially compromise such credentials resident on the system and subsequently impersonate authorized users. Related control: AC-6.

(12) *IDENTIFICATION AND AUTHENTICATION | ACCEPTANCE OF PIV CREDENTIALS*

The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials.

Supplemental Guidance: This control enhancement applies to organizations implementing logical access control systems (LACS) and physical access control systems (PACS). Personal Identity Verification (PIV) credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents. OMB Memorandum 11-11 requires federal agencies to continue implementing the requirements specified in HSPD-12 to enable agency-wide use of PIV credentials. Related controls: AU-2, PE-3, SA-4.

(13) *IDENTIFICATION AND AUTHENTICATION | OUT-OF-BAND AUTHENTICATION*

The information system implements [*Assignment: organization-defined out-of-band authentication*] under [*Assignment: organization-defined conditions*].

Supplemental Guidance: Out-of-band authentication (OOBA) refers to the use of two separate communication paths to identify and authenticate users or devices to an information system. The first path (i.e., the in-band path), is used to identify and authenticate users or devices, and generally is the path through which information flows. The second path (i.e., the out-of-band path) is used to independently verify the authentication and/or requested action. For example, a user authenticates via a notebook computer to a remote server to which the user desires access, and requests some action of the server via that communication path. Subsequently, the server contacts the user via the user's cell phone to verify that the requested action originated

Deleted: uses [*Assignment: organization-defined*

Deleted:]

Deleted: a

Deleted: authentication

Deleted: and

Deleted: a

Deleted: message. Techniques used to address this

Deleted: (e.g.,

Deleted:),

from the user. The user may either confirm the intended action to an individual on the telephone or provide an authentication code via the telephone. This type of authentication can be employed by organizations to mitigate actual or suspected man-in the-middle attacks. The conditions for activation can include, for example, suspicious activities, new threat indicators or elevated threat levels, or the impact level or classification level of information in requested transactions. Related controls: IA-10, IA-11, SC-37.

References: HSPD 12; OMB Memoranda 04-04, 06-16, 11-11; FIPS Publication 201; NIST Special Publications 800-63, 800-73, 800-76, 800-78; FICAM Roadmap and Implementation Guidance; Web: idmanagement.gov.

Priority and Baseline Allocation:

P1	**LOW** IA-2 (1)	**MOD** IA-2 (1) (2) (3) (8) (11) (12)	**HIGH** IA-2 (1) (2) (3) (4) (8) (9) (11) (12)

IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION

Control: The information system uniquely identifies and authenticates [*Assignment: organization-defined specific and/or types of devices*] before establishing a [*Selection (one or more): local; remote; network*] connection.

Supplemental Guidance: Organizational devices requiring unique device-to-device identification and authentication may be defined by type, by device, or by a combination of type/device. Information systems typically use either 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/authenticate devices on local and/or wide area networks. Organizations determine the required strength of authentication mechanisms by the security categories of information systems. Because of the challenges of applying this control on large scale, organizations are encouraged to only apply the control to those limited number (and type) of devices that truly need to support this capability. Related controls: AC-17, AC-18, AC-19, CA-3, IA-4, IA-5.

Control Enhancements:

(1) *DEVICE IDENTIFICATION AND AUTHENTICATION | CRYPTOGRAPHIC BIDIRECTIONAL AUTHENTICATION*

The information system authenticates [*Assignment: organization-defined specific devices and/or types of devices*] before establishing [*Selection (one or more): local; remote; network*] connection using bidirectional authentication that is cryptographically based.

Supplemental Guidance: A local connection is any connection with a device communicating without the use of a network. A network connection is any connection with a device that communicates through a network (e.g., local area or wide area network, Internet). A remote connection is any connection with a device communicating through an external network (e.g., the Internet). Bidirectional authentication provides stronger safeguards to validate the identity of other devices for connections that are of greater risk (e.g., remote connections). Related controls: SC-8, SC-12, SC-13.

(2) *DEVICE IDENTIFICATION AND AUTHENTICATION | CRYPTOGRAPHIC BIDIRECTIONAL NETWORK AUTHENTICATION*

[Withdrawn: Incorporated into IA-3 (1)].

(3) *DEVICE IDENTIFICATION AND AUTHENTICATION | DYNAMIC ADDRESS ALLOCATION*

The organization:

(a) Standardizes dynamic address allocation lease information and the lease duration assigned to devices in accordance with [*Assignment: organization-defined lease information and lease duration*]; and

(b) Audits lease information when assigned to a device.

Deleted: Memorandum

Deleted: *list of*

Deleted: The

Deleted: specific

Deleted: and device as deemed appropriate by the organization. The information system

Deleted: uses

Deleted: an

Deleted: solution

Deleted: and

Deleted: The

Deleted: the device

Deleted: mechanism is determined

Deleted: categorization

Deleted: the

Deleted: system

Deleted: and wireless

Deleted: connections

Deleted: between devices

Deleted: Enhancement

Deleted: Remote

Deleted: the Internet).

Deleted: AC-17, AC-18

Deleted: The information system authenticates devices before establishing network connections using bidirectional authentication between devices that is cryptographically based.

Deleted: , with regard to

Deleted: Dynamic Host Control Protocol (DHCP)

Deleted: the time assigned to devices, and audits

Supplemental Guidance: DHCP-enabled clients obtaining *leases* for IP addresses from DHCP servers, is a typical example of dynamic address allocation for devices. Related controls: AU-2, AU-3, AU-6, AU-12.

(4) *DEVICE IDENTIFICATION AND AUTHENTICATION | DEVICE ATTESTATION*

The organization ensures that device identification and authentication based on attestation is handled by [*Assignment: organization-defined configuration management process*].

Supplemental Guidance: Device attestation refers to the identification and authentication of a device based on its configuration and known operating state. This might be determined via some cryptographic hash of the device. If device attestation is the means of identification and authentication, then it is important that patches and updates to the device are handled via a configuration management process such that the those patches/updates are done securely and at the same time do not disrupt the identification and authentication to other devices.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** IA-3	**HIGH** IA-3

IA-4 IDENTIFIER MANAGEMENT

Control: The organization manages information system identifiers by:

a. Receiving authorization from [*Assignment: organization-defined personnel or roles*] to assign an individual, group, role, or device identifier;

b. Selecting an identifier that identifies an individual, group, role, or device;

c. Assigning the identifier to the intended individual, group, role, or device;

d. Preventing reuse of identifiers for [*Assignment: organization-defined time period*]; and

e. Disabling the identifier after [*Assignment: organization-defined time period of inactivity*].

Supplemental Guidance: Common device identifiers include, for example, media access control (MAC), Internet protocol (IP) addresses, or device-unique token identifiers. Management of individual identifiers is not applicable to shared information system accounts (e.g., guest and anonymous accounts). Typically, individual identifiers are the user names of the information 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 information system accounts (e.g., identifiers used in physical security control databases accessed by badge reader systems for access to information systems). Preventing reuse of identifiers implies preventing the assignment of previously used individual, group, role, or device identifiers to different individuals, groups, roles, or devices. Related controls: AC-2, IA-2, IA-3, IA-5, IA-8, SC-37.

Control Enhancements:

(1) *IDENTIFIER MANAGEMENT | PROHIBIT ACCOUNT IDENTIFIERS AS PUBLIC IDENTIFIERS*

The organization prohibits the use of information system account identifiers that are the same as public identifiers for individual electronic mail accounts.

Supplemental Guidance: Prohibiting the use of information 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 information systems. Related control: AT-2.

(2) *IDENTIFIER MANAGEMENT | SUPERVISOR AUTHORIZATION*

The organization requires that the registration process to receive an individual identifier includes supervisor authorization.

(3) *IDENTIFIER MANAGEMENT | MULTIPLE FORMS OF CERTIFICATION*

Deleted: Enhancement

Deleted: With regard to dynamic address allocation for devices,

Deleted: typically obtain

Deleted: for users and devices

Deleted: a designated organizational official

Deleted: a user

Deleted: uniquely

Deleted: user

Deleted: party or the device identifier to the intended

Deleted: user or device

Deleted: user

Deleted:) or

Deleted:

Deleted: user

Deleted: It is commonly

Deleted: case that a

Deleted: identifier is the name

Deleted: an

Deleted: account associated with an individual.

Deleted: identifier management is largely addressed by

Deleted: .

Deleted:

Deleted: covers user

Deleted: an

Deleted: account

Deleted: the identifier

Deleted: a

Deleted: database

Deleted: a

Deleted: system

Deleted: the

Deleted: system).

Deleted: control

Deleted: user

Deleted: (i.e., user identifier portion of the electronic mail address).

Deleted: Enhancement Supplemental Guidance: The organization implements this control enhancement to the extent that the information system allows.¶

Deleted: a user ID and password include authorization by a supervisor, and be ...

The organization requires multiple forms of certification of individual identification such as documentary evidence or a combination of documents and biometrics be presented to the registration authority.

Supplemental Guidance: Requiring multiple forms of identification reduces the likelihood of individuals using fraudulent identification to establish an identity, or at least increases the work factor of potential adversaries.

(4) *IDENTIFIER MANAGEMENT | IDENTIFY USER STATUS*

The organization manages individual identifiers by uniquely identifying each individual as [*Assignment: organization-defined characteristic identifying individual status*].

Supplemental Guidance: Characteristics identifying the status of individuals include, for example, contractors and foreign nationals. Identifying the status of individuals by specific characteristics provides additional information about the people with whom organizational personnel are communicating. For example, it might be useful for a government employee to know that one of the individuals on an email message is a contractor. Related control: AT-2.

(5) *IDENTIFIER MANAGEMENT | DYNAMIC MANAGEMENT*

The information system dynamically manages identifiers.

Supplemental Guidance: In contrast to conventional approaches to identification which presume static accounts for preregistered users, many distributed information systems including, for example, service-oriented architectures, rely on establishing identifiers at run time for entities that were previously unknown. In these situations, organizations anticipate and provision for the dynamic establishment of identifiers. Preestablished trust relationships and mechanisms with appropriate authorities to validate identities and related credentials are essential. Related control: AC-16.

(6) *IDENTIFIER MANAGEMENT | CROSS-ORGANIZATION MANAGEMENT*

The organization coordinates with [*Assignment: organization-defined external organizations*] for cross-organization management of identifiers.

Supplemental Guidance: Cross-organization identifier management provides the capability for organizations to appropriately identify individuals, groups, roles, or devices when conducting cross-organization activities involving the processing, storage, or transmission of information.

(7) *IDENTIFIER MANAGEMENT | IN-PERSON REGISTRATION*

The organization requires that the registration process to receive an individual identifier be conducted in person before a designated registration authority.

Supplemental Guidance: In-person registration reduces the likelihood of fraudulent identifiers being issued because it requires the physical presence of individuals and actual face-to-face interactions with designated registration authorities.

References: FIPS Publication 201; NIST Special Publications 800-73, 800-76, 800-78.

Priority and Baseline Allocation:

P1	**LOW** IA-4	**MOD** IA-4	**HIGH** IA-4

IA-5 AUTHENTICATOR MANAGEMENT

Control: The organization manages information system authenticators by:

a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;

b. Establishing initial authenticator content for authenticators defined by the organization;

c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;

d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;

Deleted: user

Deleted: the user

Deleted: *user*

Deleted: Enhancement

Deleted: user

Deleted: , attributes, and associated access authorizations

Deleted: Enhancement

Deleted: and authentication

Deleted: employ

Deleted: information system

Deleted: architecture implementations

Deleted: identities

Deleted: Dynamic

Deleted: identities and association of attributes and privileges with these identities is anticipated and provisioned. Pre-established

Deleted: for users and devices

Deleted: and/

e. Changing default content of authenticators prior to information system installation;

Deleted: upon

f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;

Deleted: (if appropriate);

g. Changing/refreshing authenticators [*Assignment: organization-defined time period by authenticator type*];

h. Protecting authenticator content from unauthorized disclosure and modification;

Deleted: and

i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and

Deleted: users…ndividuals to take, and hav …

j. Changing authenticators for group/role accounts when membership to those accounts changes.

Supplemental Guidance: Individual authenticators include, for example, passwords, tokens, biometrics, PKI certificates, and key cards. Initial authenticator content is the actual content (e.g., the initial password) as opposed to requirements about authenticator content (e.g., minimum password length). In many cases, developers ship information 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 within organizational information systems (e.g., passwords stored in hashed or encrypted formats, files containing encrypted or hashed passwords accessible with administrator privileges). Information systems support individual authenticator management by organization-defined settings and restrictions for various authenticator characteristics including, for example, minimum password length, password composition, validation time window for time synchronous one-time tokens, and number of allowed rejections during the verification stage of biometric authentication. Specific actions that can be taken to safeguard authenticators include, for example, maintaining possession of individual authenticators, not loaning or sharing individual authenticators with others, and reporting lost, stolen, or compromised authenticators immediately. Authenticator management includes issuing and revoking, when no longer needed, authenticators for temporary access such as that required for remote maintenance. Device authenticators include, for example, certificates and passwords. Related controls: AC-2, AC-3, AC-6, CM-6, IA-2, IA-4, IA-8, PL-4, PS-5, PS-6, SC-12, SC-13, SC-17, SC-28.

Deleted: User…ndividual authenticators …

Control Enhancements:

(1) *AUTHENTICATOR MANAGEMENT | PASSWORD-BASED AUTHENTICATION*

The information system, for password-based authentication:

(a) Enforces minimum password complexity of [*Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type*];

(b) Enforces at least the following number of changed characters when new passwords are created: [*Assignment: organization-defined number*];

Deleted: a [*Assignment: organization-defined*…he following number of …

(c) Stores and transmits only encrypted representations of passwords;

Deleted: Encrypts…tores and transm …

(d) Enforces password minimum and maximum lifetime restrictions of [*Assignment: organization-defined numbers for lifetime minimum, lifetime maximum*];

Deleted: and

(e) Prohibits password reuse for [*Assignment: organization-defined number*] generations; and

Deleted: .

(f) Allows the use of a temporary password for system logons with an immediate change to a permanent password.

Deleted: Enhancement

Supplemental Guidance: This control enhancement applies to single-factor authentication of individuals using passwords as individual or group authenticators, and in a similar manner, when passwords are part of multifactor authenticators. This control enhancement does *not* apply when passwords are used to unlock hardware authenticators (e.g., Personal Identity Verification cards). The implementation of such password mechanisms may not meet all of the requirements in the enhancement. Encrypted representations of passwords include, for example, encrypted versions of passwords and one-way cryptographic hashes of passwords.

Deleted: is intended primarily for environments where passwords are used as a …

The number of changed characters refers to the number of changes required with respect to the total number of positions in the current password. Password lifetime restrictions do not apply to temporary passwords. Related control: IA-6.

(2) *AUTHENTICATOR MANAGEMENT | PKI-BASED AUTHENTICATION*

The information system, for PKI-based authentication:

(a) Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information;

(b) Enforces authorized access to the corresponding private key;

(c) Maps the authenticated identity to the account of the individual or group; and

(d) Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.

Supplemental Guidance: Status information for certification paths includes, for example, certificate revocation lists or certificate status protocol responses. For PIV cards, validation of certifications involves the construction and verification of a certification path to the Common Policy Root trust anchor including certificate policy processing. Related control: IA-6.

(3) *AUTHENTICATOR MANAGEMENT | IN-PERSON OR TRUSTED THIRD-PARTY REGISTRATION*

The organization requires that the registration process to receive [*Assignment: organization-defined types of and/or specific authenticators*] be conducted [*Selection: in person; by a trusted third party*] before [*Assignment: organization-defined registration authority*] with authorization by [*Assignment: organization-defined personnel or roles*].

(4) *AUTHENTICATOR MANAGEMENT | AUTOMATED SUPPORT FOR PASSWORD STRENGTH DETERMINATION*

The organization employs automated tools to determine if password authenticators are sufficiently strong to satisfy [*Assignment: organization-defined requirements*].

Supplemental Guidance: This control enhancement focuses on the creation of strong passwords and the characteristics of such passwords (e.g., complexity) prior to use, the enforcement of which is carried out by organizational information systems in IA-5 (1). Related controls: CA-2, CA-7, RA-5.

(5) *AUTHENTICATOR MANAGEMENT | CHANGE AUTHENTICATORS PRIOR TO DELIVERY*

The organization requires developers/installers of information system components to provide unique authenticators or change default authenticators prior to delivery/installation.

Supplemental Guidance: This control enhancement extends the requirement for organizations to change default authenticators upon information 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-shelve information technology products. Requirements for unique authenticators can be included in acquisition documents prepared by organizations when procuring information systems or system components.

(6) *AUTHENTICATOR MANAGEMENT | PROTECTION OF AUTHENTICATORS*

The organization protects authenticators commensurate with the security category of the information to which use of the authenticator permits access.

Supplemental Guidance: For information 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.

(7) *AUTHENTICATOR MANAGEMENT | NO EMBEDDED UNENCRYPTED STATIC AUTHENTICATORS*

The organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.

Supplemental Guidance: Organizations exercise caution in determining whether embedded or stored authenticators are in encrypted or unencrypted form. If authenticators are used in the manner stored, then those representations are considered unencrypted authenticators. This is irrespective of whether that representation is perhaps an encrypted version of something else (e.g., a password).

(8) *AUTHENTICATOR MANAGEMENT | MULTIPLE INFORMATION SYSTEM ACCOUNTS*

Deleted: certificates

Deleted: with status information to

Deleted: and

Deleted: user

Deleted: .

Deleted: Enhancement

Deleted: online

Deleted: carried out

Deleted: a designated

Deleted: a designated organizational official (e.g., a supervisor).

Deleted: resist attacks intended to discover or otherwise compromise

Deleted: .

Deleted: vendors and/or manufacturers

Deleted: Enhancement

Deleted: vendors

Deleted: manufacturers of information system components

Deleted: those

Deleted: organization. Unique authenticators are assigned by vendors and/or manufacturers to specific information system components (i.e., delivered

Deleted:) with distinct serial numbers. This requirement is

Deleted: the organization

Deleted: and/

Deleted: information

Deleted: classification or sensitivity

Deleted: accessed

Deleted: Enhancement

Deleted: an

Deleted: authenticator is

Deleted:

Deleted: the authenticator in its stored representation, is

Deleted: that representation is

Deleted: an

Deleted: authenticator.

The organization implements [*Assignment: organization-defined security safeguards*] to manage the risk of compromise due to individuals having accounts on multiple information systems.

Supplemental Guidance: When individuals have accounts on multiple information systems, there is the risk that the compromise of one account may lead to the compromise of other accounts if individuals use the same authenticators. Possible alternatives include, for example: (i) having different authenticators on all systems; (ii) employing some form of single sign-on mechanism; or (iii) including some form of one-time passwords on all systems.

(9) *AUTHENTICATOR MANAGEMENT | CROSS-ORGANIZATION CREDENTIAL MANAGEMENT*

The organization coordinates with [*Assignment: organization-defined external organizations*] for cross-organization management of credentials.

Supplemental Guidance: Cross-organization management of credentials provides the capability for organizations to appropriately authenticate individuals, groups, roles, or devices when conducting cross-organization activities involving the processing, storage, or transmission of information.

(10) *AUTHENTICATOR MANAGEMENT | DYNAMIC CREDENTIAL ASSOCIATION*

The information system dynamically provisions identities.

Supplemental Guidance: Authentication requires some form of binding between an identity and the authenticator used to confirm the identity. In conventional approaches, this binding is established by pre-provisioning both the identity and the authenticator to the information 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 information system. New authentication techniques allow the binding between the identity and the authenticator to be implemented outside an information system. For example, with smartcard credentials, the identity and the authenticator are bound together on the card. Using these credentials, information 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. Preestablished trust relationships and mechanisms with appropriate authorities to validate identities and related credentials are essential.

(11) *AUTHENTICATOR MANAGEMENT | HARDWARE TOKEN-BASED AUTHENTICATION*

The information system, for hardware token-based authentication, employs mechanisms that satisfy [*Assignment: organization-defined token quality requirements*].

Supplemental Guidance: Hardware token-based authentication typically refers to the use of PKI-based tokens, such as the U.S. Government Personal Identity Verification (PIV) card. Organizations define specific requirements for tokens, such as working with a particular PKI.

(12) *AUTHENTICATOR MANAGEMENT | BIOMETRIC AUTHENTICATION*

The information system, for biometric-based authentication, employs mechanisms that satisfy [*Assignment: organization-defined biometric quality requirements*].

Supplemental Guidance: Unlike password-based authentication which provides exact matches of user-input passwords to stored passwords, biometric authentication does not provide such exact matches. Depending upon the type of biometric and the type of collection mechanism, there is likely to be some divergence from the presented biometric and stored biometric which serves as the basis of comparison. There will likely be both false positives and false negatives when making such comparisons. The rate at which the false accept and false reject rates are equal is known as the crossover rate. Biometric quality requirements include, for example, acceptable crossover rates, as that essentially reflects the accuracy of the biometric.

(13) *AUTHENTICATOR MANAGEMENT | EXPIRATION OF CACHED AUTHENTICATORS*

The information system prohibits the use of cached authenticators after [*Assignment: organization-defined time period*].

(14) *AUTHENTICATOR MANAGEMENT | MANAGING CONTENT OF PKI TRUST STORES*

The organization, for PKI-based authentication, employs a deliberate organization-wide methodology for managing the content of PKI trust stores installed across all platforms including networks, operating systems, browsers, and applications.

(15) *AUTHENTICATOR MANAGEMENT | FICAM-APPROVED PRODUCTS AND SERVICES*

Deleted: takes

Deleted: *measures*

Deleted: Enhancement

Deleted: an individual has

Deleted: if

Deleted: is compromised and the individual is using the same user identifier and authenticator,

Deleted: will be compromised as well.

Deleted: but are not limited to

Deleted: the same user identifier but

Deleted: having different user identifiers and authenticators on each system; (iii)

Deleted: iv

The organization uses only FICAM-approved path discovery and validation products and services.

Supplemental Guidance: Federal Identity, Credential, and Access Management (FICAM)-approved path discovery and validation products and services are those products and services that have been approved through the FICAM conformance program, where applicable.

References: OMB Memoranda 04-04, 11-11; FIPS Publication 201; NIST Special Publications 800-73, 800-63, 800-76, 800-78; FICAM Roadmap and Implementation Guidance; Web: idmanagement.gov.

Deleted: Memorandum

Priority and Baseline Allocation:

P1	**LOW** IA-5 (1) (11)	**MOD** IA-5 (1) (2) (3) (11)	**HIGH** IA-5 (1) (2) (3) (11)

IA-6 AUTHENTICATOR FEEDBACK

Control: The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

Supplemental Guidance: The feedback from information systems does not provide information that would allow unauthorized individuals to compromise authentication mechanisms. For some types of information systems or system components, for example, desktops/notebooks with relatively large monitors, the threat (often referred to as shoulder surfing) may be significant. For other types of systems or components, for example, mobile devices with 2-4 inch screens, this threat may be less significant, and may need to be balanced against the increased likelihood of typographic input errors due to the small keyboards. Therefore, the means for obscuring the authenticator feedback is selected accordingly. Obscuring the feedback of authentication information includes, for example, displaying asterisks when users type passwords into input devices, or displaying feedback for a very limited time before fully obscuring it. Related control: PE-18.

Deleted: the

Deleted: system

Deleted: an

Deleted: user

Deleted: the

Deleted: mechanism. Displaying asterisks when a user

Deleted: in a password, is an

Deleted: of

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P2	**LOW** IA-6	**MOD** IA-6	**HIGH** IA-6

Deleted: P1

IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION

Control: The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

Deleted: uses

Supplemental Guidance: Authentication mechanisms may be required within a cryptographic module to authenticate an operator accessing the module and to verify that the operator is authorized to assume the requested role and perform services within that role. Related controls: SC-12, SC-13.

Deleted: None

Control Enhancements: None.

References: FIPS Publication 140; Web: csrc.nist.gov/groups/STM/cmvp/index.html.

Deleted: -2

Deleted: CRYPTVAL

Priority and Baseline Allocation:

P1	**LOW** IA-7	**MOD** IA-7	**HIGH** IA-7

IA-8 IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)

Control: The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).

Supplemental Guidance: Non-organizational users include information system users other than organizational users explicitly covered by IA-2. These individuals are uniquely identified and authenticated for accesses other than those accesses explicitly identified and documented in AC-14. In accordance with the E-Authentication E-Government initiative, authentication of non-organizational users accessing federal information systems may be required to protect federal, proprietary, or privacy-related information (with exceptions noted for national security systems). Organizations use risk assessments to determine authentication needs and consider scalability, practicality, and security in balancing the need to ensure ease of use for access to federal information and information systems with the need to protect and adequately mitigate risk. IA-2 addresses identification and authentication requirements for access to information systems by organizational users. Related controls: AC-2, AC-14, AC-17, AC-18, IA-2, IA-4, IA-5, MA-4, RA-3, SA-12, SC-8.

Control Enhancements:

(1) *IDENTIFICATION AND AUTHENTICATION | ACCEPTANCE OF PIV CREDENTIALS FROM OTHER AGENCIES*

The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies.

Supplemental Guidance: This control enhancement applies to logical access control systems (LACS) and physical access control systems (PACS). Personal Identity Verification (PIV) credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents. OMB Memorandum 11-11 requires federal agencies to continue implementing the requirements specified in HSPD-12 to enable agency-wide use of PIV credentials. Related controls: AU-2, PE-3, SA-4.

(2) *IDENTIFICATION AND AUTHENTICATION | ACCEPTANCE OF THIRD-PARTY CREDENTIALS*

The information system accepts only FICAM-approved third-party credentials.

Supplemental Guidance: This control enhancement typically applies to organizational information systems that are accessible to the general public, for example, public-facing websites. Third-party credentials are those credentials issued by nonfederal government entities approved by the Federal Identity, Credential, and Access Management (FICAM) Trust Framework Solutions initiative. Approved third-party credentials meet or exceed the set of minimum federal government-wide technical, security, privacy, and organizational maturity requirements. This allows federal government relying parties to trust such credentials at their approved assurance levels. Related control: AU-2.

(3) *IDENTIFICATION AND AUTHENTICATION | USE OF FICAM-APPROVED PRODUCTS*

The organization employs only FICAM-approved information system components in [*Assignment: organization-defined information systems*] to accept third-party credentials.

Supplemental Guidance: This control enhancement typically applies to information systems that are accessible to the general public, for example, public-facing websites. FICAM-approved information system components include, for example, information technology products and software libraries that have been approved by the Federal Identity, Credential, and Access Management conformance program. Related control: SA-4.

(4) *IDENTIFICATION AND AUTHENTICATION | USE OF FICAM-ISSUED PROFILES*

The information system conforms to FICAM-issued profiles.

Supplemental Guidance: This control enhancement addresses open identity management standards. To ensure that these standards are viable, robust, reliable, sustainable (e.g., available in commercial information technology products), and interoperable as documented,

Deleted: all

Deleted: Users

Deleted: all

Deleted: by the organization in accordance with

Deleted:

Deleted: Accordingly, a

Deleted: assessment is used in determining the

Deleted: of the organization. Scalability

Deleted: are simultaneously considered

Deleted: to organizational operations, organizational assets, individuals, other organizations, and the Nation. Identification

Deleted: system access

Deleted: are described in IA-2.

Deleted: ¶

the United States Government assesses and scopes identity management standards and technology implementations against applicable federal legislation, directives, policies, and requirements. The result is FICAM-issued implementation profiles of approved protocols (e.g., FICAM authentication protocols such as SAML 2.0 and OpenID 2.0, as well as other protocols such as the FICAM Backend Attribute Exchange). Related control: SA-4.

(5) *IDENTIFICATION AND AUTHENTICATION | ACCEPTANCE OF PIV-I CREDENTIALS*

The information system accepts and electronically verifies Personal Identity Verification-I (PIV-I) credentials.

Supplemental Guidance: This control enhancement: (i) applies to logical and physical access control systems; and (ii) addresses Non-Federal Issuers (NFIs) of identity cards that desire to interoperate with United States Government Personal Identity Verification (PIV) information systems and that can be trusted by federal government-relying parties. The X.509 certificate policy for the Federal Bridge Certification Authority (FBCA) addresses PIV-I requirements. The PIV-I card is suitable for Assurance Level 4 as defined in OMB Memorandum 04-04 and NIST Special Publication 800-63, and multifactor authentication as defined in NIST Special Publication 800-116. PIV-I credentials are those 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 (directly or through another PKI bridge) with the FBCA with policies that have been mapped and approved as meeting the requirements of the PIV-I policies defined in the FBCA certificate policy. Related control: AU-2.

References: OMB Memoranda 04-04, 11-11, 10-06-2011; FICAM Roadmap and Implementation Guidance; FIPS Publication 201; NIST Special Publications 800-63, 800-116; National Strategy for Trusted Identities in Cyberspace; Web: idmanagement.gov.

Deleted: WWW.CIO.GOV/EAUTHENTICATION;

Priority and Baseline Allocation:

P1	**LOW** IA-8 (1) (2) (3) (4)	**MOD** IA-8 (1) (2) (3) (4)	**HIGH** IA-8 (1) (2) (3) (4)

IA-9 SERVICE IDENTIFICATION AND AUTHENTICATION

Control: The organization identifies and authenticates [*Assignment: organization-defined information system services*] using [*Assignment: organization-defined security safeguards*].

Supplemental Guidance: This control supports service-oriented architectures and other distributed architectural approaches requiring the identification and authentication of information system services. In such architectures, external services often appear dynamically. Therefore, information systems should be able to determine in a dynamic manner, if external providers and associated services are authentic. Safeguards implemented by organizational information systems to validate provider and service authenticity include, for example, information or code signing, provenance graphs, and/or electronic signatures indicating or including the sources of services.

Control Enhancements:

(1) *SERVICE IDENTIFICATION AND AUTHENTICATION | INFORMATION EXCHANGE*

The organization ensures that service providers receive, validate, and transmit identification and authentication information.

(2) *SERVICE IDENTIFICATION AND AUTHENTICATION | TRANSMISSION OF DECISIONS*

The organization ensures that identification and authentication decisions are transmitted between [*Assignment: organization-defined services*] consistent with organizational policies.

Supplemental Guidance: For distributed architectures (e.g., service-oriented architectures), the decisions regarding the validation of identification and authentication claims may be made by services separate from the services acting on those decisions. In such situations, it is necessary to provide the identification and authentication decisions (as opposed to the actual identifiers and authenticators) to the services that need to act on those decisions. Related control: SC-8.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

IA-10 ADAPTIVE IDENTIFICATION AND AUTHENTICATION

Control: The organization requires that individuals accessing the information system employ [*Assignment: organization-defined supplemental authentication techniques or mechanisms*] under specific [*Assignment: organization-defined circumstances or situations*].

Supplemental Guidance: Adversaries may compromise individual authentication mechanisms and subsequently attempt to impersonate legitimate users. This situation can potentially occur with any authentication mechanisms employed by organizations. To address this threat, organizations may employ specific techniques/mechanisms and establish protocols to assess suspicious behavior (e.g., individuals accessing information that they do not typically access as part of their normal duties, roles, or responsibilities, accessing greater quantities of information than the individuals would routinely access, or attempting to access information from suspicious network addresses). In these situations when certain preestablished conditions or triggers occur, organizations can require selected individuals to provide additional authentication information. Another potential use for adaptive identification and authentication is to increase the strength of mechanism based on the number and/or types of records being accessed. Related controls: AU-6, SI-4.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

IA-11 RE-AUTHENTICATION

Control: The organization requires users and devices to re-authenticate when [*Assignment: organization-defined circumstances or situations requiring re-authentication*].

Supplemental Guidance: In addition to the re-authentication requirements associated with session locks, organizations may require re-authentication of individuals and/or devices in other situations including, for example: (i) when authenticators change; (ii), when roles change; (iii) when security categories of information systems change; (iv), when the execution of privileged functions occurs; (v) after a fixed period of time; or (vi) periodically. Related control: AC-11.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

FAMILY: INCIDENT RESPONSE

Deleted:
CLASS: OPERATIONAL

IR-1 INCIDENT RESPONSE POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and

b. Reviews and updates the current:

1. Incident response policy [*Assignment: organization-defined frequency*]; and

2. Incident response procedures [*Assignment: organization-defined frequency*].

Deleted: develops,

Deleted: , and reviews/updates

Deleted: *frequency*

Deleted: A formal, documented

Deleted: Formal, documented procedures

Deleted: .

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the IR family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Deleted: is intended to produce

Deleted: that are required

Deleted: incident response

Deleted: The policy

Deleted: are consistent with

Deleted: policies,

Deleted: Existing organizational

Deleted: additional

Deleted:

Deleted: incident response

Deleted: the organization. Incident response

Deleted: developed

Deleted: a

Deleted: system, when required.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-61, 800-83, 800-100.

Priority and Baseline Allocation:

P1	**LOW** IR-1	**MOD** IR-1	**HIGH** IR-1

IR-2 INCIDENT RESPONSE TRAINING

Control: The organization provides incident response training to information system users consistent with assigned roles and responsibilities:

a. Within [*Assignment: organization-defined time period*] of assuming an incident response role or responsibility;

b. When required by information system changes; and

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

Deleted: Provides refresher training

Deleted:].

Supplemental Guidance: Incident response training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure the appropriate content and level of detail is included in such training. For example, regular users may only need to know who to call or how to recognize an incident on the information system; system administrators may require additional training on how to handle/remediate incidents; and incident responders may receive more specific training on forensics, reporting, system recovery, and restoration. Incident response training includes user training in the identification and reporting of suspicious activities, both from external and internal sources. Related controls: AT-3, CP-3, IR-8.

Deleted:

Deleted: control

Control Enhancements:

(1) *INCIDENT RESPONSE TRAINING | SIMULATED EVENTS*

The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.

(2) *INCIDENT RESPONSE TRAINING | AUTOMATED TRAINING ENVIRONMENTS*

The organization employs automated mechanisms to provide a more thorough and realistic incident response training environment.

References: NIST Special Publications 800-16, 800-50.

Priority and Baseline Allocation:

P2	**LOW** IR-2	**MOD** IR-2	**HIGH** IR-2 (1) (2)

IR-3 INCIDENT RESPONSE TESTING

Deleted: AND EXERCISES

Control: The organization tests the incident response capability for the information system [*Assignment: organization-defined frequency*] using [*Assignment: organization-defined tests*] to determine the incident response effectiveness and documents the results.

Deleted: and/or exercises

Deleted: *and/or exercises*

Supplemental Guidance: Organizations test incident response capabilities to determine the overall effectiveness of the capabilities and to identify potential weaknesses or deficiencies. Incident response testing includes, for example, the use of checklists, walk-through or tabletop exercises, simulations (parallel/full interrupt), and comprehensive exercises. Incident response testing can also include a determination of the effects on organizational operations (e.g., reduction in mission capabilities), organizational assets, and individuals due to incident response. Related controls: CP-4, IR-8.

Deleted: None.

Control Enhancements:

(1) *INCIDENT RESPONSE TESTING | AUTOMATED TESTING*

The organization employs automated mechanisms to more thoroughly and effectively test the incident response capability.

Deleted: /exercise

Supplemental Guidance: Organizations use automated mechanisms to more thoroughly and effectively test incident response capabilities, for example: (i) by providing more complete coverage of incident response issues; (ii) by selecting more realistic test scenarios and test environments; and (iii) by stressing the response capability. Related control: AT-2.

Deleted: Enhancement

Deleted: Automated

Deleted: can provide the ability

Deleted: or exercise the

Deleted: capability

Deleted: ,

Deleted: /exercise

Deleted: ,

Deleted: more effectively

Deleted:

(2) *INCIDENT RESPONSE TESTING | COORDINATION WITH RELATED PLANS*

The organization coordinates incident response testing with organizational elements responsible for related plans.

Supplemental Guidance: Organizational plans related to incident response testing include, for example, Business Continuity Plans, Contingency Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, and Occupant Emergency Plans.

References: NIST Special Publications 800-84, 800-115.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** IR-3 (2)	**HIGH** IR-3 (2)

Deleted: (1)

IR-4 INCIDENT HANDLING

Control: The organization:

a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;

b. Coordinates incident handling activities with contingency planning activities; and

c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

Supplemental Guidance: Organizations recognize that incident response capability is dependent on the capabilities of organizational information 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 information 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, information system owners, authorizing officials, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices, and the risk executive (function). Related controls: AU-6, CM-6, CP-2, CP-4, IR-2, IR-3, IR-8, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7.

Deleted: but not limited to,

Deleted: and

Deleted: .

Control Enhancements:

(1) *INCIDENT HANDLING | AUTOMATED INCIDENT HANDLING PROCESSES*

The organization employs automated mechanisms to support the incident handling process.

Supplemental Guidance: Automated mechanisms supporting incident handling processes include, for example, online incident management systems.

Deleted: Enhancement

Deleted: An

Deleted: system is an example of an automated mechanism

(2) *INCIDENT HANDLING | DYNAMIC RECONFIGURATION*

The organization includes dynamic reconfiguration of *[Assignment: organization-defined information system components]* as part of the incident response capability.

Deleted: the

Supplemental Guidance: Dynamic reconfiguration includes, for example, changes to router rules, access control lists, intrusion detection/prevention system parameters, and filter rules for firewalls and gateways. Organizations perform dynamic reconfiguration of information 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 information systems in the definition of the reconfiguration capability, considering the potential need for rapid response in order to effectively address sophisticated cyber threats. Related controls: AC-2, AC-4, AC-16, CM-2, CM-3, CM-4.

Deleted: Enhancement

(3) *INCIDENT HANDLING | CONTINUITY OF OPERATIONS*

The organization identifies *[Assignment: organization-defined classes of incidents]* and *[Assignment: organization-defined actions to take in response to classes of incidents]* to ensure continuation of organizational missions and business functions.

Deleted: defines appropriate

Supplemental Guidance: Classes of incidents include, for example, malfunctions due to design/implementation errors and omissions, targeted malicious attacks, and untargeted malicious attacks. Appropriate incident response actions include, for example, graceful degradation, information 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.

Deleted: Enhancement

Deleted: Incident

Deleted: that may be appropriate

Deleted: or

Deleted: (e.g., false data flows, false status measures),

Deleted: a system is

(4) *INCIDENT HANDLING | INFORMATION CORRELATION*

The organization correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.

Supplemental Guidance: Sometimes the nature of a threat event, for example, a hostile cyber 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.

(5) *INCIDENT HANDLING | AUTOMATIC DISABLING OF INFORMATION SYSTEM*

The organization implements a configurable capability to automatically disable the information system if *[Assignment: organization-defined security violations]* are detected.

Deleted: any of the following security violations are detected:

Deleted: ***list of***

(6) *INCIDENT HANDLING | INSIDER THREATS - SPECIFIC CAPABILITIES*

The organization implements incident handling capability for insider threats.

Supplemental Guidance: While many organizations address insider threat incidents as an inherent part of their organizational incident response capability, this control enhancement provides additional emphasis on this type of threat and the need for specific incident handling capabilities (as defined within organizations) to provide appropriate and timely responses.

(7) *INCIDENT HANDLING | INSIDER THREATS - INTRA-ORGANIZATION COORDINATION*

The organization coordinates incident handling capability for insider threats across [*Assignment: organization-defined components or elements of the organization*].

Supplemental Guidance: Incident handling for insider threat incidents (including preparation, detection and analysis, containment, eradication, and recovery) requires close coordination among a variety of organizational components or elements to be effective. These components or elements include, for example, mission/business owners, information 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.

(8) *INCIDENT HANDLING | CORRELATION WITH EXTERNAL ORGANIZATIONS*

The organization coordinates with [*Assignment: organization-defined external organizations*] to correlate and share [*Assignment: organization-defined incident information*] to achieve a cross-organization perspective on incident awareness and more effective incident responses.

Supplemental Guidance: The coordination of incident information with external organizations including, for example, mission/business partners, military/coalition partners, customers, and multitiered 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.

(9) *INCIDENT HANDLING | DYNAMIC RESPONSE CAPABILITY*

The organization employs [*Assignment: organization-defined dynamic response capabilities*] to effectively respond to security incidents.

Supplemental Guidance: This control enhancement addresses the deployment of replacement or new capabilities in a timely manner in response to security incidents (e.g., adversary actions during hostile cyber attacks). This includes capabilities implemented at the mission/business process level (e.g., activating alternative mission/business processes) and at the information system level. Related control: CP-10.

(10) *INCIDENT HANDLING | SUPPLY CHAIN COORDINATION*

The organization coordinates incident handling activities involving supply chain events with other organizations involved in the supply chain.

Supplemental Guidance: Organizations involved in supply chain activities include, for example, system/product developers, integrators, manufacturers, packagers, assemblers, distributors, vendors, and resellers. Supply chain incidents include, for example, compromises/breaches involving information system components, information technology products, development processes or personnel, and distribution processes or warehousing facilities.

References: Executive Order 13587; NIST Special Publication 800-61.

Priority and Baseline Allocation:

P1	**LOW** IR-4	**MOD** IR-4 (1)	**HIGH** IR-4 (1) (4)

IR-5 INCIDENT MONITORING

Control: The organization tracks and documents information system security incidents.

Supplemental Guidance: Documenting information system security incidents includes, for example, maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources including, for example, incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. Related controls: AU-6, IR-8, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7.

Deleted:

Control Enhancements:

(1) *INCIDENT MONITORING | AUTOMATED TRACKING / DATA COLLECTION / ANALYSIS*

The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

Supplemental Guidance: Automated mechanisms for tracking security incidents and collecting/analyzing incident information include, for example, the Einstein network monitoring device and monitoring online Computer Incident Response Centers (CIRCs) or other electronic databases of incidents. Related controls: AU-7, IR-4.

Deleted: Enhancement

Deleted: 6, AU-

Deleted: SI

References: NIST Special Publication 800-61.

Priority and Baseline Allocation:

P1	**LOW** IR-5	**MOD** IR-5	**HIGH** IR-5 (1)

IR-6 INCIDENT REPORTING

Control: The organization:

a. Requires personnel to report suspected security incidents to the organizational incident response capability within [*Assignment: organization-defined time period*]; and

b. Reports security incident information to [*Assignment: organization-defined authorities*].

Deleted: -

Deleted: designated

Deleted: .

Supplemental Guidance: The intent of this control is to address both specific incident reporting requirements within an organization and the formal incident reporting requirements for federal agencies and their subordinate organizations. Suspected security incidents include, for example, the receipt of suspicious email communications that can potentially contain malicious code. The types of security incidents reported, the content and timeliness of the reports, and the designated reporting authorities reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Current federal policy requires that all federal agencies (unless specifically exempted from such requirements) report security incidents to the United States Computer Emergency Readiness Team (US-CERT) within specified time frames designated in the US-CERT Concept of Operations for Federal Cyber Security Incident Handling. Related controls: IR-4, IR-5, IR-8.

Deleted: list of

Deleted: are consistent with

Deleted: policies,

Deleted:

Deleted:

Control Enhancements:

(1) *INCIDENT REPORTING | AUTOMATED REPORTING*

The organization employs automated mechanisms to assist in the reporting of security incidents.

Supplemental Guidance: Related control: IR-7.

(2) *INCIDENT REPORTING | VULNERABILITIES RELATED TO INCIDENTS*

The organization reports information system vulnerabilities associated with reported security incidents to [*Assignment: organization-defined personnel or roles*].

Deleted: weaknesses, deficiencies, and/or

(3) *INCIDENT REPORTING | COORDINATION WITH SUPPLY CHAIN*

The organization provides security incident information to other organizations involved in the supply chain for information systems or information system components related to the incident.

Supplemental Guidance: Organizations involved in supply chain activities include, for example, system/product developers, integrators, manufacturers, packagers, assemblers, distributors, vendors, and resellers. Supply chain incidents include, for example, compromises/breaches involving information system components, information technology products, development processes or personnel, and distribution processes or warehousing facilities. Organizations determine the appropriate information to share considering the value gained from support by external organizations with the potential for harm due to sensitive information being released to outside organizations of perhaps questionable trustworthiness.

Deleted: organizational officials

References: NIST Special Publication 800-61: Web: www.us-cert.gov.

Priority and Baseline Allocation:

P1	**LOW** IR-6	**MOD** IR-6 (1)	**HIGH** IR-6 (1)

IR-7 INCIDENT RESPONSE ASSISTANCE

Control: The organization provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

Deleted: ,

Supplemental Guidance: Incident response support resources provided by organizations include, for example, help desks, assistance groups, and access to forensics services, when required. Related controls: AT-2, IR-4, IR-6, IR-8, SA-9.

Deleted: Possible implementations of incident

Deleted: in an organization

Deleted: a

Deleted: desk or an

Deleted: group

Deleted:

Control Enhancements:

(1) *INCIDENT RESPONSE ASSISTANCE | AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION / SUPPORT*

The organization employs automated mechanisms to increase the availability of incident response-related information and support.

Supplemental Guidance: Automated mechanisms can provide a push and/or pull capability for users to obtain incident response assistance. For example, individuals might have access to a website to query the assistance capability, or conversely, the assistance capability may have the ability to proactively send information to users (general distribution or targeted) as part of increasing understanding of current response capabilities and support.

Deleted: Enhancement

Deleted:

(2) *INCIDENT RESPONSE ASSISTANCE | COORDINATION WITH EXTERNAL PROVIDERS*

The organization:

(a) Establishes a direct, cooperative relationship between its incident response capability and external providers of information system protection capability; and

(b) Identifies organizational incident response team members to the external providers.

Supplemental Guidance: External providers of information 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.

Deleted: Enhancement

References: None.

Priority and Baseline Allocation:

P2	**LOW** IR-7	**MOD** IR-7 (1)	**HIGH** IR-7 (1)

Deleted: P3

IR-8 INCIDENT RESPONSE PLAN

Control: The organization:

a. Develops an incident response plan that:

1. Provides the organization with a roadmap for implementing its incident response capability;

2. Describes the structure and organization of the incident response capability;

3. Provides a high-level approach for how the incident response capability fits into the overall organization;

4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;

5. Defines reportable incidents;

6. Provides metrics for measuring the incident response capability within the organization;

7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and

8. Is reviewed and approved by [*Assignment:* *organization-defined personnel or roles*];

b. Distributes copies of the incident response plan to [*Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements*];

c. Reviews the incident response plan [*Assignment: organization-defined frequency*];

d. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;

e. Communicates incident response plan changes to [*Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements*]; and

f. Protects the incident response plan from unauthorized disclosure and modification.

Supplemental Guidance: It is important that organizations develop and implement a coordinated approach to incident response. Organizational missions, business functions, strategies, goals, and objectives for incident response help to determine the structure of incident response capabilities. As part of a comprehensive incident response capability, organizations consider the coordination and sharing of information with external organizations, including, for example, external service providers and organizations involved in the supply chain for organizational information systems. Related controls: MP-2, MP-4, MP-5.

Control Enhancements: None.

References: NIST Special Publication 800-61.

Priority and Baseline Allocation:

P1	**LOW** IR-8	**MOD** IR-8	**HIGH** IR-8

IR-9 INFORMATION SPILLAGE RESPONSE

Control: The organization responds to information spills by:

a. Identifying the specific information involved in the information system contamination;

b. Alerting [*Assignment: organization-defined personnel or roles*] of the information spill using a method of communication not associated with the spill;

c. Isolating the contaminated information system or system component;

d. Eradicating the information from the contaminated information system or component;

e. Identifying other information systems or system components that may have been subsequently contaminated; and

f. Performing other [*Assignment: organization-defined actions*].

Deleted: .

Deleted: designated officials within the

Deleted: ;

Deleted: *list of*

Deleted: Revises

Deleted: and

Deleted: *list of*

Deleted:].

Deleted: have

Deleted: formal, focused, and

Deleted: responding to incidents. The organization’s mission

Deleted: and

Deleted: its

Deleted: develops, disseminates,

Supplemental Guidance: Information spillage refers to instances where either classified or sensitive information is inadvertently placed on information systems that are not authorized to process such information. Such information spills often occur when information that is initially thought to be of lower sensitivity is transmitted to an information system and then is subsequently determined to be of higher sensitivity. At that point, corrective action is required. The nature of the organizational response is generally based upon the degree of sensitivity of the spilled information (e.g., security category or classification level), the security capabilities of the information system, the specific nature of contaminated storage media, and the access authorizations (e.g., security clearances) of individuals with authorized access to the contaminated system. The methods used to communicate information about the spill after the fact do not involve methods directly associated with the actual spill to minimize the risk of further spreading the contamination before such contamination is isolated and eradicated.

Control Enhancements:

(1) *INFORMATION SPILLAGE RESPONSE | RESPONSIBLE PERSONNEL*

Deleted: reviews/updates

The organization assigns [*Assignment: organization-defined personnel or roles*] with responsibility for responding to information spills.

(2) *INFORMATION SPILLAGE RESPONSE | TRAINING*

The organization provides information spillage response training [*Assignment: organization-defined frequency*].

(3) *INFORMATION SPILLAGE RESPONSE | POST-SPILL OPERATIONS*

The organization implements [*Assignment: organization-defined procedures*] to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions.

Supplemental Guidance: Correction actions for information 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.

(4) *INFORMATION SPILLAGE RESPONSE | EXPOSURE TO UNAUTHORIZED PERSONNEL*

The organization employs [*Assignment: organization-defined security safeguards*] for personnel exposed to information not within assigned access authorizations.

Supplemental Guidance: Security safeguards include, for example, making personnel exposed to spilled information aware of the federal laws, directives, policies, and/or regulations regarding the information and the restrictions imposed based on exposure to such information.

References: None.

Moved (insertion) [9]

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

IR-10 INTEGRATED INFORMATION SECURITY ANALYSIS TEAM

Control: The organization establishes an integrated team of forensic/malicious code analysts, tool developers, and real-time operations personnel.

Supplemental Guidance: Having an integrated team for incident response facilitates information sharing. Such capability allows organizational personnel, including developers, implementers, and operators, to leverage the team knowledge of the threat in order to implement defensive measures that will enable organizations to deter intrusions more effectively. Moreover, it promotes 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 security analysis team can rapidly develop an appropriate response for operators to implement, correlate the new incident with information on past intrusions, and augment ongoing intelligence development. This enables the team to identify adversary TTPs that are linked to the operations tempo or to specific missions/business functions, and to define responsive actions in a way that does not disrupt the mission/business operations. Ideally, information security analysis teams are distributed within organizations to make the capability more resilient.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

FAMILY: MAINTENANCE

MA-1 SYSTEM MAINTENANCE POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

1. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; and

Deleted: Formal, documented procedures

Deleted: information

Deleted: .

b. Reviews and updates the current:

1. System maintenance policy [*Assignment: organization-defined frequency*]; and

2. System maintenance procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the MA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Deleted: is intended to produce

Deleted: that are required

Deleted: system maintenance

Deleted: The policy

Deleted: are consistent with

Deleted: policies,

Deleted: Existing organizational

Deleted: additional

Deleted:

Deleted: information system maintenance

Deleted: the organization. System maintenance

Deleted: developed

Deleted: a

Deleted: system, when required.

Deleted: the development of the system maintenance

Control Enhancements: None.

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

Priority and Baseline Allocation:

P1	**LOW** MA-1	**MOD** MA-1	**HIGH** MA-1

MA-2 CONTROLLED MAINTENANCE

Control: The organization:

a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements;

b. Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;

Deleted: Controls

c. Requires that [*Assignment: organization-defined personnel or roles*] explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;

Deleted: a designated official

d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs;

Deleted: and

e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and

f. Includes [*Assignment: organization-defined maintenance-related information*] in organizational maintenance records.

Supplemental Guidance: This control addresses the information security aspects of the information system maintenance program and applies to all types of maintenance to any system component (including applications) conducted by any local or nonlocal entity (e.g., in-contract, warranty, in-house, software maintenance agreement). System maintenance also includes those components not directly associated with information processing and/or data/information retention such as scanners, copiers, and printers. Information necessary for creating effective maintenance records includes, for example: (i) date and time of maintenance; (ii) name of individuals or group performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance performed; and (v) information system components/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 information systems. Organizations consider supply chain issues associated with replacement components for information systems. Related controls: CM-3, CM-4, MA-4, MP-6, PE-16, SA-12, SI-2.

Control Enhancements:

(1) *CONTROLLED MAINTENANCE | RECORD CONTENT*

[Withdrawn: Incorporated into MA-2].

(2) *CONTROLLED MAINTENANCE | AUTOMATED MAINTENANCE ACTIVITIES*

The organization:

(a) Employs automated mechanisms to schedule, conduct, and document maintenance and repairs; and

(b) Produces up-to date, accurate, and complete records of all maintenance and repair actions requested, scheduled, in process, and completed.

Supplemental Guidance: Related controls: CA-7, MA-3.

References: None.

Priority and Baseline Allocation:

P2	**LOW** MA-2	**MOD** MA-2	**HIGH** MA-2 (2)

MA-3 MAINTENANCE TOOLS

Control: The organization approves, controls, and monitors information system maintenance tools.

Supplemental Guidance: This control addresses security-related issues associated with maintenance tools used specifically for diagnostic and repair actions on organizational information systems. Maintenance tools can include hardware, software, and firmware items. Maintenance tools are potential vehicles for transporting malicious code, either intentionally or unintentionally, into a facility and subsequently into organizational information systems. Maintenance tools can include, for example, hardware/software diagnostic test equipment and hardware/software packet sniffers. This control does not cover hardware/software components that may support information system maintenance, yet are a part of the system, for example, the software implementing “ping,” “ls,” “ipconfig,” or the hardware and software implementing the monitoring port of an Ethernet switch. Related controls: MA-2, MA-5, MP-6.

Control Enhancements:

(1) *MAINTENANCE TOOLS | INSPECT TOOLS*

The organization inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.

Supplemental Guidance: If, upon inspection of maintenance tools, organizations determine that the tools have been modified in an improper/unauthorized manner or contain malicious code,

Deleted: The

Deleted: is intended to address

Deleted: organization’s

Deleted: A

Deleted: The organization maintains maintenance records for the information system that include:¶
<#>Date and time of maintenance;¶
<#>Name of the individual performing the maintenance;¶
<#>Name of escort, if necessary;¶
<#>A description of the maintenance performed; and¶
<#>A list of equipment removed or replaced (including identification numbers, if applicable).¶

Deleted: employs

Deleted: as required, producing

Deleted: , and available

Deleted: , needed

Deleted: (1)

Deleted: (1)

Deleted: the use of, and maintains on an ongoing basis,

Deleted: The intent of this

Deleted: is to address the

Deleted: arising from the hardware and software brought into the information system

Deleted: (e.g., a

Deleted: or

Deleted: sniffer that is introduced for the purpose of a particular maintenance activity). Hardware and/or

Deleted: (e.g.,

Deleted:) are not covered by this control.

Deleted: control:

Deleted: all

Deleted: obvious

Deleted: Enhancement

Deleted: Maintenance tools include, for example, diagnostic and test equipment used to conduct maintenance on the information system.

the incident is handled consistent with organizational policies and procedures for incident handling. Related control: SI-7.

(2) *MAINTENANCE TOOLS | INSPECT MEDIA*

The organization checks media containing diagnostic and test programs for malicious code before the media are used in the information system.

Deleted: all

Supplemental Guidance: If, upon inspection of media containing maintenance diagnostic and test programs, organizations determine that the media contain malicious code, the incident is handled consistent with organizational incident handling policies and procedures. Related control: SI-3.

(3) *MAINTENANCE TOOLS | PREVENT UNAUTHORIZED REMOVAL*

The organization prevents the unauthorized removal of maintenance equipment containing organizational information by:

Deleted: one of the following: (i) verifying

(a) Verifying that there is no organizational information contained on the equipment;

Deleted: (ii) sanitizing

(b) Sanitizing or destroying the equipment;

Deleted: (iii) retaining

(c) Retaining the equipment within the facility; or

Deleted: (iv) obtaining

(d) Obtaining an exemption from [*Assignment: organization-defined personnel or roles*] explicitly authorizing removal of the equipment from the facility.

Deleted: a designated

Deleted: official

Supplemental Guidance: Organizational information includes all information specifically owned by organizations and information provided to organizations in which organizations serve as information stewards.

(4) *MAINTENANCE TOOLS | RESTRICTED TOOL USE*

The information system restricts the use of maintenance tools to authorized personnel only.

Deleted: organization employs automated mechanisms to restrict

Supplemental Guidance: This control enhancement applies to information systems that are used to carry out maintenance functions. Related controls: AC-2, AC-3, AC-5, AC-6.

References: NIST Special Publication 800-88.

Priority and Baseline Allocation:

P3	**LOW** Not Selected	**MOD** MA-3 (1) (2)	**HIGH** MA-3 (1) (2) (3)

Deleted: P2

MA-4 NONLOCAL MAINTENANCE

Deleted: NON-LOCAL

Control: The organization:

a. Approves and monitors nonlocal maintenance and diagnostic activities;

Deleted: Authorizes,

Deleted: , and controls

b. Allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system;

c. Employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions;

Deleted: identification and authentication techniques

d. Maintains records for nonlocal maintenance and diagnostic activities; and

e. Terminates session and network connections when nonlocal maintenance is completed.

Deleted: all sessions

Supplemental Guidance: Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through a network, either an external network (e.g., the Internet) or an internal network. Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the information system or information 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. Typically, 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.

Deleted:

Deleted: Identification and authentication

Deleted: are consistent with

Enforcing requirements in MA-4 is accomplished in part by other controls. Related controls: AC-2, AC-3, AC-6, AC-17, AU-2, AU-3, IA-2, IA-4, IA-5, IA-8, MA-2, MA-5, MP-6, PL-2, SC-7, SC-10, SC-17.

Control Enhancements:

(1) *NONLOCAL MAINTENANCE | AUDITING AND REVIEW*

The organization:

(a) Audits nonlocal maintenance and diagnostic sessions [*Assignment: organization-defined audit events*]; and

(b) Reviews the records of the maintenance and diagnostic sessions.

Supplemental Guidance: Related controls: AU-2, AU-6, AU-12.

(2) *NONLOCAL MAINTENANCE | DOCUMENT NONLOCAL MAINTENANCE*

The organization documents in the security plan for the information system, the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.

(3) *NONLOCAL MAINTENANCE | COMPARABLE SECURITY / SANITIZATION*

The organization:

(a) Requires that nonlocal maintenance and diagnostic services be performed from an information system that implements a security capability comparable to the capability implemented on the system being serviced; or

(b) Removes the component to be serviced from the information system and prior to nonlocal maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software) before reconnecting the component to the information system.

Supplemental Guidance: Comparable security capability on information 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 information system being serviced. Related controls: MA-3, SA-12, SI-3, SI-7.

(4) *NONLOCAL MAINTENANCE | AUTHENTICATION / SEPARATION OF MAINTENANCE SESSIONS*

The organization protects nonlocal maintenance sessions by:

(a) Employing [*Assignment: organization-defined authenticators that are replay resistant*]; and

(b) Separating the maintenance sessions from other network sessions with the information system by either:

(1) Physically separated communications paths; or

(2) Logically separated communications paths based upon encryption.

Supplemental Guidance: Related control: SC-13.

(5) *NONLOCAL MAINTENANCE | APPROVALS AND NOTIFICATIONS*

The organization:

(a) Requires the approval of each nonlocal maintenance session by [*Assignment: organization-defined personnel or roles*]; and

(b) Notifies [*Assignment: organization-defined personnel or roles*] of the date and time of planned nonlocal maintenance.

Supplemental Guidance: Notification may be performed by maintenance personnel. Approval of nonlocal maintenance sessions is accomplished by organizational personnel with sufficient information security and information system knowledge to determine the appropriateness of the proposed maintenance.

(6) *NONLOCAL MAINTENANCE | CRYPTOGRAPHIC PROTECTION*

The information system implements cryptographic mechanisms to protect the integrity and confidentiality of nonlocal maintenance and diagnostic communications.

Supplemental Guidance: Related controls: SC-8, SC-13.

(7) *NONLOCAL MAINTENANCE | REMOTE DISCONNECT VERIFICATION*

Deleted:

Deleted: ,

Deleted: audits

Deleted: and designated organizational personnel review

Deleted: maintenance

Deleted: ,

Deleted: installation

Deleted: non-local

Deleted: non-local

Deleted: level of

Deleted: at least as high as that

Deleted: non-local

Deleted: and surreptitious implants

Deleted: through the use of a strong authenticator tightly bound to the user and

Deleted: Enhancement

Deleted: Maintenance personnel

Deleted: notify

Deleted: A designated

Deleted: official

Deleted: with specific information security/information system knowledge approves the non-local

Deleted:] when non-local maintenance is

Deleted: (i.e., date/time); and

Deleted: /

Deleted: organization employs

Deleted: non-local

The information system implements remote disconnect verification at the termination of nonlocal maintenance and diagnostic sessions.

Supplemental Guidance: Remote disconnect verification ensures that remote connections from nonlocal maintenance sessions have been terminated and are no longer available for use. Related control: SC-13.

References: FIPS Publications 140-2, 197, 201; NIST Special Publications 800-63, 800-88; CNSS Policy 15.

Priority and Baseline Allocation:

P2	**LOW** MA-4	**MOD** MA-4 (2)	**HIGH** MA-4 (2) (3)

MA-5 MAINTENANCE PERSONNEL

Control: The organization:

a. Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel;

b. Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and

c. Designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

Supplemental Guidance: This control applies to individuals performing hardware or software maintenance on organizational information systems, while PE-2 addresses physical access for individuals whose maintenance duties place them within the physical protection perimeter of the systems (e.g., custodial staff, physical plant maintenance personnel). Technical competence of supervising individuals relates to the maintenance performed on the information 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 information systems, for example, when required to conduct maintenance activities with little or no notice. Based on organizational assessments of risk, organizations may issue temporary credentials to these individuals. Temporary credentials may be for one-time use or for very limited time periods. Related controls: AC-2, IA-8, MP-2, PE-2, PE-3, PE-4, RA-3.

Control Enhancements:

(1) *MAINTENANCE PERSONNEL | INDIVIDUALS WITHOUT APPROPRIATE ACCESS*

The organization:

(a) Implements procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements:

(1) Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified;

(2) Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the information system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and

(b) Develops and implements alternate security safeguards in the event an information system component cannot be sanitized, removed, or disconnected from the system.

Deleted: organization employs

Deleted: non-local

Deleted: P1

Deleted: 1) (

Deleted: 1) (

Deleted: current

Deleted: and

Deleted: or designates

Deleted: deemed necessary

Deleted: information system

Deleted: when maintenance

Deleted: in the information system

Deleted: vendor personnel

Deleted: legitimately

Deleted: the system

Deleted: or diagnostic

Deleted:

Deleted: a prior assessment

Deleted: the organization

Deleted:

Deleted: a

Deleted: period.

Deleted: MA-5

Deleted: maintains

Deleted: In the

Deleted: the procedures contained in the security plan for

Deleted: are enforced

Supplemental Guidance: This control enhancement denies individuals who lack appropriate security clearances (i.e., individuals who do not possess security clearances or possess security clearances at a lower level than required) or who are not U.S. citizens, visual and electronic access to any classified information, Controlled Unclassified Information (CUI), or any other sensitive information contained on organizational information systems. Procedures for the use of maintenance personnel can be documented in security plans for the information systems. Related controls: MP-6, PL-2.

Deleted: Enhancement
Deleted: The intent of this
Deleted: is to deny
Deleted: the
Deleted: system.
Deleted: the
Deleted: plan
Deleted: system

(2) *MAINTENANCE PERSONNEL | SECURITY CLEARANCES FOR CLASSIFIED SYSTEMS*

The organization ensures that personnel performing maintenance and diagnostic activities on an information system processing, storing, or transmitting classified information possess security clearances and formal access approvals for at least the highest classification level and for all compartments of information on the system.

Supplemental Guidance: Related control: PS-3.

Deleted: are cleared (i.e.,
Deleted: appropriate
Deleted:)

(3) *MAINTENANCE PERSONNEL | CITIZENSHIP REQUIREMENTS FOR CLASSIFIED SYSTEMS*

The organization ensures that personnel performing maintenance and diagnostic activities on an information system processing, storing, or transmitting classified information are U.S. citizens.

Supplemental Guidance: Related control: PS-3.

(4) *MAINTENANCE PERSONNEL | FOREIGN NATIONALS*

The organization ensures that:

(a) Cleared foreign nationals (i.e., foreign nationals with appropriate security clearances), are used to conduct maintenance and diagnostic activities on classified information systems only when the systems are jointly owned and operated by the United States and foreign allied governments, or owned and operated solely by foreign allied governments; and

(b) Approvals, consents, and detailed operational conditions regarding the use of foreign nationals to conduct maintenance and diagnostic activities on classified information systems are fully documented within Memoranda of Agreements.

Supplemental Guidance: Related control: PS-3.

Deleted: an
Deleted: system
Deleted: system is
Deleted: an
Deleted: system
Deleted: a Memorandum
Deleted: Agreement

(5) *MAINTENANCE PERSONNEL | NONSYSTEM-RELATED MAINTENANCE*

The organization ensures that non-escorted personnel performing maintenance activities not directly associated with the information system but in the physical proximity of the system, have required access authorizations.

Supplemental Guidance: Personnel performing maintenance activities in other capacities not directly related to the information system include, for example, physical plant personnel and janitorial personnel.

References: None.

Priority and Baseline Allocation:

P2	**LOW** MA-5	**MOD** MA-5	**HIGH** MA-5 (1)

Deleted: P1

MA-6 TIMELY MAINTENANCE

Control: The organization obtains maintenance support and/or spare parts for [*Assignment: organization-defined information system components*] within [*Assignment: organization-defined time period*] of failure.

Supplemental Guidance: Organizations specify the information system components that result in increased risk to organizational operations and assets, individuals, other organizations, or the Nation when the functionality provided by those components is not operational. Organizational actions to obtain maintenance support typically include having appropriate contracts in place. Related controls: CM-8, CP-2, CP-7, SA-14, SA-15.

Control Enhancements:

Deleted: *list of security-critical*
Deleted: *components and/or key information technology*
Deleted: The organization specifies those
Deleted: , when not operational,
Deleted: individuals,
Deleted: because
Deleted: security
Deleted: intended by that component is not being
Deleted: . Security-critical
Deleted: None.

(1) *TIMELY MAINTENANCE | PREVENTIVE MAINTENANCE*

The organization performs preventive maintenance on [*Assignment: organization-defined information system components*] at [*Assignment: organization-defined time intervals*].

Supplemental Guidance: Preventive maintenance includes proactive care and servicing of organizational information systems components for the purpose of maintaining 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 actually fail. Methods of determining what preventive (or other) failure management policies to apply include, for example, original equipment manufacturer (OEM) 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.

Deleted: firewalls, guards, gateways, intrusion detection systems, audit repositories, authentication servers, and intrusion prevention systems. Related

(2) *TIMELY MAINTENANCE | PREDICTIVE MAINTENANCE*

The organization performs predictive maintenance on [*Assignment: organization-defined information system components*] at [*Assignment: organization-defined time intervals*].

Supplemental Guidance: Predictive maintenance, or condition-based maintenance, attempts to evaluate the condition of equipment by performing periodic or continuous (online) equipment condition monitoring. The goal of predictive maintenance is to perform maintenance at a scheduled point in time when the maintenance activity is most cost-effective and before the equipment loses performance within a threshold. The predictive component of predictive maintenance stems from the goal of predicting the future trend of the equipment's condition. This approach uses principles of statistical process control to determine at what point in the future maintenance activities will be appropriate. Most predictive maintenance inspections are performed while equipment is in service, thereby minimizing disruption of normal system operations. Predictive maintenance can result in substantial cost savings and higher system reliability. Predictive maintenance tends to include measurement of the item. To evaluate equipment condition, predictive maintenance utilizes nondestructive testing technologies such as infrared, acoustic (partial discharge and airborne ultrasonic), corona detection, vibration analysis, sound level measurements, oil analysis, and other specific online tests.

(3) *TIMELY MAINTENANCE | AUTOMATED SUPPORT FOR PREDICTIVE MAINTENANCE*

The organization employs automated mechanisms to transfer predictive maintenance data to a computerized maintenance management system.

Supplemental Guidance: A computerized maintenance management system maintains a computer database of information about the maintenance operations of organizations and automates processing equipment condition data in order to trigger maintenance planning, execution, and reporting.

References: None.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** MA-6	**HIGH** MA-6

Deleted: P1

FAMILY: MEDIA PROTECTION

MP-1 MEDIA PROTECTION POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls; and

b. Reviews and updates the current:

1. Media protection policy [*Assignment: organization-defined frequency*]; and

2. Media protection procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the MP family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

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

Priority and Baseline Allocation:

P1	**LOW** MP-1	**MOD** MP-1	**HIGH** MP-1

MP-2 MEDIA ACCESS

Control: The organization restricts access to [*Assignment: organization-defined types of digital and/or non-digital media*] to [*Assignment: organization-defined personnel or roles*].

Supplemental Guidance: Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Restricting non-digital media access includes, for example, denying access to patient medical records in a community hospital unless the individuals seeking access to such records are authorized healthcare providers. Restricting access to digital media includes, for example, limiting access to design specifications stored on compact disks in the media library to the project leader and the individuals on the development team. Related controls: AC-3, IA-2, MP-4, PE-2, PE-3, PL-2.

Control Enhancements:

(1) *MEDIA ACCESS | AUTOMATED RESTRICTED ACCESS*

[Withdrawn: Incorporated into MP-4 (2)].

(2) *MEDIA ACCESS | CRYPTOGRAPHIC PROTECTION*

Deleted:
CLASS: OPERATIONAL

Deleted: develops,

Deleted: , and reviews/updates

Deleted: *frequency*

Deleted: A formal, documented

Deleted: Formal, documented procedures

Deleted: .

Deleted: is intended to produce

Deleted: that are required

Deleted: media protection

Deleted: The policy

Deleted: are consistent with

Deleted: policies,

Deleted: Existing organizational

Deleted: additional

Deleted:

Deleted: media protection

Deleted: the organization. Media protection

Deleted: developed

Deleted: a

Deleted: system, when required.

Deleted: the development of the media protection

Deleted: .

Deleted: *list of authorized individuals*] using [*Assignment: organization-defined security measures*

Deleted: media (e.g.,

Deleted: /thumb

Deleted:) and non-digital media (e.g., paper, microfilm). This control also applies to mobile computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal

Deleted: assistants, cellular telephones,

Deleted: cameras, and audio recording devices). An organizational assessment of risk guides the selection of media and associated information contained on that

Deleted: requiring restricted access. Organizations document in policy and procedures, the media requiring restricted

Deleted: ,

Deleted: authorized to

Deleted: the media, and the specific measure ...

Deleted: . Fewer protection measures are ...

Deleted: The organization employs ...

[Withdrawn: Incorporated into SC-28 (1)].

References: FIPS Publication 199; NIST Special Publication 800-111.

Priority and Baseline Allocation:

P1	**LOW** MP-2	**MOD** MP-2	**HIGH** MP-2

MP-3 MEDIA MARKING

Control: The organization:

a. Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and

b. Exempts [*Assignment: organization-defined types of information system media*] from marking as long as the media remain within [*Assignment: organization-defined controlled areas*].

Supplemental Guidance: The term *security marking* refers to the application/use of human-readable security attributes. The term *security labeling* refers to the application/use of security attributes with regard to internal data structures within information systems (see AC-16). Information 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. 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 information system media reflects applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Related controls: AC-16, PL-2, RA-3.

Control Enhancements: None.

References: FIPS Publication 199.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** MP-3	**HIGH** MP-3

MP-4 MEDIA STORAGE

Control: The organization:

a. Physically controls and securely stores [*Assignment: organization-defined types of digital and/or non-digital media*] within [*Assignment: organization-defined controlled areas*]; and

b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

Supplemental Guidance: Information 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. Physically controlling information 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 all stored media. Secure storage includes, for example, a locked drawer, desk, or cabinet, or a controlled media library. The type of media storage is commensurate with the security category and/or classification of the information residing on the media. Controlled areas are areas for which organizations provide sufficient physical and procedural safeguards to meet the requirements established for

Deleted: The information system uses cryptographic mechanisms to protect and restrict access to information on portable digital media.¶

Deleted: (1)

Deleted: (1)

Deleted: , in accordance with organizational policies and procedures, removable

Deleted: and information system output

Deleted: *list*

Deleted: *removable*

Deleted: *types*

Deleted: exempted items

Deleted: is used when referring

Deleted: or

Deleted:

Deleted: is used when referring

Deleted: or

Deleted: the

Deleted: system

Deleted: , Security Attributes). Removable ...

Deleted: media (e.g.,

Deleted: /thumb

Deleted:) and non-digital media (e.g., paper ...

Deleted: requiring

Deleted: . Marking

Deleted: the organization

Deleted: Some

Deleted: , however,

Deleted: Organizations may extend the scop ...

Deleted: P1

Deleted:] using [*Assignment: organization* ...

Deleted: media (e.g.,

Deleted: /thumb

Deleted:) and non

Deleted: (e.g.,

Deleted: ,

Deleted:). This control also applies

Deleted: mobile computing and ...

Deleted: capability (e.g., notebook/laptop ...

Deleted: systems and may have the capabilit ...

Deleted: internal media (e.g., on voicemail ...

Deleted: the organization has confidence tha ...

Deleted: protections are sufficient

protecting information and/or information systems. For media containing information determined by organizations to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on organizations or individuals if accessed by other than authorized personnel, fewer safeguards may be needed. In these situations, physical access controls provide adequate protection. Related controls: CP-6, CP-9, MP-2, MP-7, PE-3.

Control Enhancements:

(1) *MEDIA STORAGE | CRYPTOGRAPHIC PROTECTION*

[Withdrawn: Incorporated into SC-28 (1)].

(2) *MEDIA STORAGE | AUTOMATED RESTRICTED ACCESS*

The organization employs automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted.

Supplemental Guidance: Automated mechanisms can include, for example, keypads on the external entries to media storage areas. Related controls: AU-2, AU-9, AU-6, AU-12.

References: FIPS Publication 199; NIST Special Publications 800-56, 800-57, 800-111.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** MP-4	**HIGH** MP-4

MP-5 MEDIA TRANSPORT

Control: The organization:

a. Protects and controls [*Assignment: organization-defined types of information system media*] during transport outside of controlled areas using [*Assignment: organization-defined security safeguards*];

b. Maintains accountability for information system media during transport outside of controlled areas;

c. Documents activities associated with the transport of information system media; and

d. Restricts the activities associated with the transport of information system media to authorized personnel.

Supplemental Guidance: Information 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. This control also applies to mobile devices with information storage capability (e.g., smart phones, tablets, E-readers), that are transported outside of controlled areas. Controlled areas are areas or spaces for which organizations provide sufficient physical and/or procedural safeguards to meet the requirements established for protecting information and/or information systems.

Physical and technical safeguards for media are commensurate with the security category or classification of the information residing on the media. Safeguards to protect media during transport include, for example, locked containers and cryptography. Cryptographic mechanisms can provide confidentiality and integrity protections depending upon the mechanisms used. Activities associated with transport include the actual transport as well as those activities such as releasing media for transport and ensuring that media enters the appropriate transport processes. For the actual transport, authorized transport and courier personnel may include individuals from outside the organization (e.g., U.S. Postal Service or a commercial transport or delivery service). Maintaining accountability of media during transport includes, for example, restricting transport activities to authorized personnel, and tracking and/or obtaining explicit records of transport activities as the media moves through the transportation system to prevent and detect loss,

Deleted: the information and/or information system.

Deleted: An organizational assessment of risk guides the selection of media and associated information contained on that media requiring physical protection. Fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on the organization or individuals if accessed by other than authorized personnel. In these situations, it is assumed that the physical access controls to the facility where the media resides provide adequate protection.¶
As part of a defense-in-depth strategy, the organization considers routinely encrypting information at rest on selected secondary storage devices. The employment of cryptography is at the discretion of the information owner/steward. The selection of the cryptographic mechanisms used is based upon maintaining the confidentia …

Deleted: The organization employs …

Deleted: *digital and non-digital*

Deleted: *measures*

Deleted: and

Deleted: such

Deleted: media (e.g.,

Deleted: /thumb

Deleted:) and non

Deleted: (e.g.,

Deleted: ,

Deleted:).

Deleted: computing and communications

Deleted: notebook/laptop computers, persona …

Deleted: Telephone systems

Deleted: also considered information system …

Deleted: space

Deleted: the organization has confidence tha …

Deleted: protections provided are sufficient

Deleted: the

Deleted: system

Deleted: security measures

Deleted: the protection of digital and non- …

Deleted: or sensitivity

Deleted: , and consistent with applicable fed …

Deleted: are examples of security measures …

Deleted: /or

Deleted: An organizational assessment of ris …

Deleted: requiring protection during transpor …

Deleted: . Authorized

destruction, or tampering. Organizations establish documentation requirements for activities associated with the transport of information system media in accordance with organizational assessments of risk to include the flexibility to define different record-keeping methods for the different types of media transport as part of an overall system of transport-related records. Related controls: AC-19, CP-9, MP-3, MP-4, RA-3, SC-8, SC-13, SC-28.

Control Enhancements:

(1) *MEDIA TRANSPORT | PROTECTION OUTSIDE OF CONTROLLED AREAS*

[Withdrawn: Incorporated into MP-5].

(2) *MEDIA TRANSPORT | DOCUMENTATION OF ACTIVITIES*

[Withdrawn: Incorporated into MP-5].

(3) *MEDIA TRANSPORT | CUSTODIANS*

The organization employs an identified custodian during transport of information system media outside of controlled areas.

Supplemental Guidance: Identified custodians provide organizations with specific points of contact during the media transport process and facilitate individual accountability. Custodial responsibilities can be transferred from one individual to another as long as an unambiguous custodian is identified at all times.

(4) *MEDIA TRANSPORT | CRYPTOGRAPHIC PROTECTION*

The information system implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

Supplemental Guidance: This control enhancement applies to both portable storage devices (e.g., USB memory sticks, compact disks, digital video disks, external/removable hard disk drives) and mobile devices with storage capability (e.g., smart phones, tablets, E-readers). Related control: MP-2.

References: FIPS Publication 199; NIST Special Publication 800-60.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** MP-5 (4)	**HIGH** MP-5 (4)

MP-6 MEDIA SANITIZATION

Control: The organization:

a. Sanitizes [*Assignment: organization-defined* information system media] prior to disposal, release out of organizational control, or release for reuse using [*Assignment: organization-defined sanitization techniques and procedures*] in accordance with applicable federal and organizational standards and policies; and

b. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

Supplemental Guidance: This control applies to all information system media, both digital and non-digital, subject to disposal or reuse, whether or not the media is considered removable. Examples include media found in scanners, copiers, printers, notebook computers, workstations, network components, and mobile devices. 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.

Deleted: the

Deleted: assessment

Deleted: The organization documents activities associated with the transport of information system media.¶
Enhancement Supplemental Guidance: Organizations establish documentation requirements for activities associated with the transport of information system media in accordance with the organizational assessment of risk to include the flexibility to define different record-keeping methods for different types of media transport as part of an overall system of transport-related records.¶

Deleted: throughout the

Deleted: Enhancement

Deleted: organization employs

Deleted: Enhancement

Deleted: also

Deleted: mobile devices. Mobile devices include

Deleted: media

Deleted: portable computing and communications

Deleted: notebook/laptop computers, personal digital assistants, cellular telephones).

Deleted: 4. Related controls: MP-

Deleted: ; SC-13

Deleted: 2) (

Deleted: 2) (3) (

Deleted: sanitizes

Deleted: , both digital and non-digital,

Deleted: .

Deleted: Sanitization is the

Deleted: used to remove

Deleted: information system

Deleted: there is reasonable assurance that

Deleted:

Deleted: and destroying media information

Deleted: organizational

Deleted: The organization employs sanitization mechanisms with strength and integrity commensurate with the classification or sensitivity of the information. The organization uses its

Deleted: the organization

Sanitization of non-digital media includes, for example, removing a classified appendix from an otherwise unclassified document, or redacting selected sections or words from a document by obscuring the redacted sections/words in a manner equivalent in effectiveness to removing them from the document. NSA standards and policies control the sanitization process for media containing classified information. Related controls: MA-2, MA-4, RA-3, SC-4.

Control Enhancements:

(1) *MEDIA SANITIZATION | REVIEW / APPROVE / TRACK / DOCUMENT / VERIFY*

The organization reviews, approves, tracks, documents, and verifies media sanitization and disposal actions.

Supplemental Guidance: Organizations review and approve media to be sanitized to ensure compliance with records-retention policies. Tracking/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 disposal action taken. Organizations verify that the sanitization of the media was effective prior to disposal. Related control: SI-12.

(2) *MEDIA SANITIZATION | EQUIPMENT TESTING*

The organization tests sanitization equipment and procedures [*Assignment: organization-defined frequency*] to verify that the intended sanitization is being achieved.

Supplemental Guidance: Testing of sanitization equipment and procedures may be conducted by qualified and authorized external entities (e.g., other federal agencies or external service providers).

(3) *MEDIA SANITIZATION | NONDESTRUCTIVE TECHNIQUES*

The organization applies nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the information system under the following circumstances: [*Assignment: organization-defined circumstances requiring sanitization of portable storage devices*].

Supplemental Guidance: This control enhancement applies to digital media containing classified information and Controlled Unclassified Information (CUI). Portable storage devices can be the source of malicious code insertions into organizational information systems. Many of these devices are obtained from unknown and potentially untrustworthy sources and may contain malicious code that can be readily transferred to information systems through USB ports or other entry portals. While scanning such storage devices is always recommended, sanitization provides additional assurance that the devices are free of malicious code to include code capable of initiating zero-day attacks. Organizations consider nondestructive sanitization of portable storage devices when such devices are first purchased from the manufacturer or vendor prior to initial use or when organizations lose a positive chain of custody for the devices. Related control: SI-3.

(4) *MEDIA SANITIZATION | CONTROLLED UNCLASSIFIED INFORMATION*

[Withdrawn: Incorporated into MP-6].

(5) *MEDIA SANITIZATION | CLASSIFIED INFORMATION*

[Withdrawn: Incorporated into MP-6].

(6) *MEDIA SANITIZATION | MEDIA DESTRUCTION*

[Withdrawn: Incorporated into MP-6].

(7) *MEDIA SANITIZATION | DUAL AUTHORIZATION*

The organization enforces dual authorization for the sanitization of [*Assignment: organization-defined information system media*].

Deleted: to verify correct performance

Deleted: sanitizes

Deleted: , removable

Deleted: ***list of***

Deleted: ***, removable***

Deleted: Enhancement

Deleted: , removable

Deleted: (e.g., thumb drives, flash drives, external storage devices)

Deleted:

Deleted: various types of

Deleted: the

Deleted: system

Deleted:

Deleted: device is

Deleted: all

Deleted: , removable

Deleted: , for example,

Deleted: the organization loses

Deleted: device. An organizational assessment of risk guides the specific circumstances for employing the sanitization process.

Deleted: The organization sanitizes information system media containing Controlled Unclassified Information (CUI) or other sensitive information in accordance with applicable organizational and/or federal standards and policies.

Deleted: The organization sanitizes information system media containing classified information in accordance with NSA standards and policies.

Deleted: The organization destroys information system media that cannot be sanitized.

Supplemental Guidance: Organizations employ dual authorization to ensure that information system media sanitization cannot occur unless two technically qualified individuals conduct the task. Individuals sanitizing information system media possess sufficient skills/expertise to determine if the proposed sanitization reflects applicable federal/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. Related controls: AC-3, MP-2.

(8) *MEDIA SANITIZATION | REMOTE PURGING / WIPING OF INFORMATION*

The organization provides the capability to purge/wipe information from [*Assignment: organization-defined information systems, system components, or devices*] either remotely or under the following conditions: [*Assignment: organization-defined conditions*].

Supplemental Guidance: This control enhancement protects data/information on organizational information systems, system components, or devices (e.g., mobile devices) if such systems, components, or devices are obtained by unauthorized individuals. Remote purge/wipe commands require strong authentication to mitigate the risk of unauthorized individuals purging/wiping the system/component/device. The purge/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.

References: FIPS Publication 199; NIST Special Publications 800-60, 800-88; Web: www.nsa.gov/ia/mitigation_guidance/media_destruction_guidance/index.shtml.

Priority and Baseline Allocation:

P1	**LOW** MP-6	**MOD** MP-6	**HIGH** MP-6 (1) (2) (3)

MP-7 MEDIA USE

Control: The organization [*Selection: restricts; prohibits*] the use of [*Assignment: organization-defined types of information system media*] on [*Assignment: organization-defined information systems or system components*] using [*Assignment: organization-defined security safeguards*].

Supplemental Guidance: Information 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. This control also applies to mobile devices with information storage capability (e.g., smart phones, tablets, E-readers). In contrast to MP-2, which restricts user access to media, this control restricts the use of certain types of media on information systems, for example, restricting/prohibiting the use of flash drives or external hard disk drives. Organizations can employ technical and nontechnical safeguards (e.g., policies, procedures, rules of behavior) to restrict the use of information 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/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. Related controls: AC-19, PL-4.

Control Enhancements:

(1) *MEDIA USE | PROHIBIT USE WITHOUT OWNER*

The organization prohibits the use of portable storage devices in organizational information systems when such devices have no identifiable owner.

Supplemental Guidance: Requiring identifiable owners (e.g., individuals, organizations, or projects) for portable storage devices reduces the risk of using such technologies by allowing

Deleted: Section Break (Next Page)

Deleted: develops, disseminates,

organizations to assign responsibility and accountability for addressing known vulnerabilities in the devices (e.g., malicious code insertion). Related control: PL-4.

Deleted: reviews/updates

(2) *MEDIA USE | PROHIBIT USE OF SANITIZATION-RESISTANT MEDIA*

The organization prohibits the use of sanitization-resistant media in organizational information systems.

Supplemental Guidance: Sanitation-resistance 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. Sanitation-resistant media include, for example, compact flash, embedded flash on boards and devices, solid state drives, and USB removable media. Related control: MP-6.

References: FIPS Publication 199; NIST Special Publication 800-111.

Priority and Baseline Allocation:

P1	**LOW** MP-7	**MOD** MP-7 (1)	**HIGH** MP-7 (1)

MP-8 MEDIA DOWNGRADING

Control: The organization:

a. Establishes [*Assignment: organization-defined information system media downgrading process*] that includes employing downgrading mechanisms with [*Assignment: organization-defined strength and integrity*];

b. Ensures that the information system media downgrading process is commensurate with the security category and/or classification level of the information to be removed and the access authorizations of the potential recipients of the downgraded information;

c. Identifies [*Assignment: organization-defined information system media requiring downgrading*]; and

d. Downgrades the identified information system media using the established process.

Supplemental Guidance: This control applies to all information system media, digital and non-digital, subject to release outside of the organization, whether or not the media is considered removable. The downgrading process, when applied to system media, removes information from the media, typically by security category or classification level, such that the information cannot be retrieved or reconstructed. Downgrading of media includes redacting information to enable wider release and distribution. Downgrading of media also ensures that empty space on the media (e.g., slack space within files) is devoid of information.

Control Enhancements:

(1) *MEDIA DOWNGRADING | DOCUMENTATION OF PROCESS*

The organization documents information system media downgrading actions.

Supplemental Guidance: Organizations can document the media downgrading process by providing information such as the downgrading technique employed, the identification number of the downgraded media, and the identity of the individual that authorized and/or performed the downgrading action.

(2) *MEDIA DOWNGRADING | EQUIPMENT TESTING*

The organization employs [*Assignment: organization-defined tests*] of downgrading equipment and procedures to verify correct performance [*Assignment: organization-defined frequency*].

(3) *MEDIA DOWNGRADING | CONTROLLED UNCLASSIFIED INFORMATION*

The organization downgrades information system media containing [*Assignment: organization-defined Controlled Unclassified Information (CUI)*] prior to public release in accordance with applicable federal and organizational standards and policies.

(4) *MEDIA DOWNGRADING | CLASSIFIED INFORMATION*

The organization downgrades information system media containing classified information prior to release to individuals without required access authorizations in accordance with NSA standards and policies.

Supplemental Guidance: Downgrading of classified information uses approved sanitization tools, techniques, and procedures to transfer information confirmed to be unclassified from classified information systems to unclassified media.

References: None.

Moved (insertion) [10]

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION

PE-1 PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

1. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and

Deleted: Formal, documented procedures

Deleted: .

b. Reviews and updates the current:

1. Physical and environmental protection policy [*Assignment: organization-defined frequency*]; and

2. Physical and environmental protection procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PE family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Deleted: is intended to produce

Deleted: that are required

Deleted: physical and environmental protection

Deleted: The policy

Deleted: are consistent with

Deleted: policies,

Deleted: Existing organizational

Deleted: additional

Deleted:

Deleted: physical and environmental protection

Deleted: the organization. Physical and environmental protection

Deleted: developed

Deleted: a

Deleted: system, when required.

Deleted: the development of the physical and environmental protection

Deleted: .

Control Enhancements: None.

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

Priority and Baseline Allocation:

P1	**LOW** PE-1	**MOD** PE-1	**HIGH** PE-1

PE-2 PHYSICAL ACCESS AUTHORIZATIONS

Control: The organization:

a. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides;

b. Issues authorization credentials for facility access;

c. Reviews the access list detailing authorized facility access by individuals [*Assignment: organization-defined frequency*]; and

d. Removes individuals from the facility access list when access is no longer required.

Deleted: keeps current

Deleted: personnel

Deleted: (except for those areas within the facility officially designated as publicly accessible);

Deleted: and approves

Deleted: and authorization credentials

Deleted:], removing

Deleted: personnel

Deleted: requiring access

Supplemental Guidance: This control applies to organizational employees and visitors. Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors. Authorization credentials include, for example, badges, identification cards, and smart cards. Organizations determine the strength of authorization credentials needed (including level of forge-proof badges, smart cards, or identification cards) consistent with federal standards, policies, and procedures. This control only applies to areas within facilities that have not been designated as publicly accessible. Related controls: PE-3, PE-4, PS-3.

Deleted: control

Control Enhancements:

(1) *PHYSICAL ACCESS AUTHORIZATIONS | ACCESS BY POSITION / ROLE*

The organization authorizes physical access to the facility where the information system resides based on position or role.

Supplemental Guidance: Related controls: AC-2, AC-3, AC-6.

(2) *PHYSICAL ACCESS AUTHORIZATIONS | TWO FORMS OF IDENTIFICATION*

The organization requires two forms of identification from [*Assignment: organization-defined list of acceptable forms of identification*] for visitor access to the facility where the information system resides.

Deleted: to gain

Supplemental Guidance: Acceptable forms of government photo identification include, for example, passports, Personal Identity Verification (PIV) cards, and drivers' licenses. In the case of gaining access to facilities using automated mechanisms, organizations may use PIV cards, key cards, PINs, and biometrics. Related controls: IA-2, IA-4, IA-5.

Deleted: Enhancement

Deleted: Examples of

Deleted: are identification badge

Deleted: card, cipher PIN

(3) *PHYSICAL ACCESS AUTHORIZATIONS | RESTRICT UNESCORTED ACCESS*

The organization restricts unescorted access to the facility where the information system resides to personnel with [*Selection (one or more): security clearances for all information contained within the system; formal access authorizations for all information contained within the system; need for access to all information contained within the system; [Assignment: organization-defined credentials*]].

Deleted: physical

Deleted: containing an

Deleted: that processes

Supplemental Guidance: Due to the highly sensitive nature of classified information stored within certain facilities, it is important that individuals lacking sufficient security clearances, access approvals, or need to know, be escorted by individuals with appropriate credentials to ensure that such information is not exposed or otherwise compromised. Related controls: PS-2, PS-6.

References: None.

Priority and Baseline Allocation:

P1	**LOW** PE-2	**MOD** PE-2	**HIGH** PE-2

PE-3 PHYSICAL ACCESS CONTROL

Control: The organization:

a. Enforces physical access authorizations at [*Assignment: organization-defined entry/exit points to the facility where the information system resides*] by;

1. Verifying individual access authorizations before granting access to the facility; and

2. Controlling ingress/egress to the facility using [*Selection (one or more): [Assignment: organization-defined physical access control systems/devices*]; guards];

b. Maintains physical access audit logs for [*Assignment: organization-defined entry/exit points*];

c. Provides [*Assignment: organization-defined security safeguards*] to control access to areas within the facility officially designated as publicly accessible;

d. Escorts visitors and monitors visitor activity [*Assignment: organization-defined circumstances requiring visitor escorts and monitoring*];

Deleted: for all physical access points (including designated

Deleted:)

Deleted: (excluding those areas within the facility officially designated as publicly accessible);

Deleted: Verifies

Deleted: Controls entry

Deleted: containing the information system

Deleted: devices and/or guards;

Deleted: Controls

Deleted: in accordance with the organization's assessment of risk

e. Secures keys, combinations, and other physical access devices;

f. Inventories [*Assignment: organization-defined physical access devices*] every [*Assignment: organization-defined frequency*]; and

g. Changes combinations and keys [*Assignment: organization-defined frequency*] and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.

Supplemental Guidance: This control applies to organizational employees and visitors. Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors. Organizations determine the types of facility guards needed including, for example, professional physical security staff or other personnel such as administrative staff or information system users. Physical access devices include, for example, keys, locks, combinations, and card readers. Safeguards for publicly accessible areas within organizational facilities include, for example, cameras, monitoring by guards, and isolating selected information systems and/or system components in secured areas. Physical access control systems comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The Federal Identity, Credential, and Access Management Program provides implementation guidance for identity, credential, and access management capabilities for physical access control systems. Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural (e.g., a written log of individuals accessing the facility and when such access occurred), automated (e.g., capturing ID provided by a PIV card), or some combination thereof. Physical access points can include facility access points, interior access points to information systems and/or components requiring supplemental access controls, or both. Components of organizational information systems (e.g., workstations, terminals) may be located in areas designated as publicly accessible with organizations safeguarding access to such devices. Related controls: AU-2, AU-6, MP-2, MP-4, PE-2, PE-4, PE-5, PS-3, RA-3.

Control Enhancements:

(1) *PHYSICAL ACCESS CONTROL | INFORMATION SYSTEM ACCESS*

The organization enforces physical access authorizations to the information system in addition to the physical access controls for the facility at [*Assignment: organization-defined physical spaces containing one or more components of the information system*].

Supplemental Guidance: This control enhancement provides additional physical security for those areas within facilities where there is a concentration of information system components (e.g., server rooms, media storage areas, data and communications centers). Related control: PS-2.

(2) *PHYSICAL ACCESS CONTROL | FACILITY / INFORMATION SYSTEM BOUNDARIES*

The organization performs security checks [*Assignment: organization-defined frequency*] at the physical boundary of the facility or information system for unauthorized exfiltration of information or removal of information system components.

Supplemental Guidance: Organizations determine the extent, frequency, and/or randomness of security checks to adequately mitigate risk associated with exfiltration. Related controls: AC-4, SC-7.

(3) *PHYSICAL ACCESS CONTROL | CONTINUOUS GUARDS / ALARMS / MONITORING*

The organization employs guards and/or alarms to monitor every physical access point to the facility where the information system resides 24 hours per day, 7 days per week.

Supplemental Guidance: Related controls: CP-6, CP-7.

(4) *PHYSICAL ACCESS CONTROL | LOCKABLE CASINGS*

The organization uses lockable physical casings to protect [*Assignment: organization-defined information system components*] from unauthorized physical access.

(5) *PHYSICAL ACCESS CONTROL | TAMPER PROTECTION*

The organization employs [*Assignment: organization-defined security safeguards*] to [*Selection (one or more): detect; prevent*] physical tampering or alteration of [*Assignment: organization-defined hardware components*] within the information system.

Supplemental Guidance: Organizations may implement tamper detection/prevention at selected hardware components or tamper detection at some components and tamper prevention at other components. Tamper detection/prevention activities can employ many types of anti-tamper technologies including, for example, tamper-detection seals and anti-tamper coatings. Anti-tamper programs help to detect hardware alterations through counterfeiting and other supply chain-related risks. Related control: SA-12.

Deleted: Supplemental Guidance: The organization determines

Deleted: , as deemed appropriate.

Deleted: Workstations and associated peripherals connected to (and part

Deleted:) an organizational information system

Deleted: being safeguarded.

Deleted: independent of

Deleted: .

Deleted: Enhancement

Deleted: applies to server rooms, media storage areas, communications centers, or any other areas within an organizational facility containing large concentrations of information system components. The intent is to provide

Deleted: where the organization may be more vulnerable due to the

Deleted: . Security requirements for facilities containing organizational information systems that process, store, or transmit Sensitive Compartmented Information (SCI) are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards,

Deleted: guidance. See also

Deleted: 3, security requirements for personnel

Deleted: to SCI.

Deleted: Enhancement

Deleted: The

Deleted: /

Deleted:

Deleted: the

Deleted: is as deemed necessary by the organization

Deleted: , alarms,

Deleted: monitors

Deleted: information system detects/prevents

(6) *PHYSICAL ACCESS CONTROL | FACILITY PENETRATION TESTING*

The organization employs a penetration testing process that includes [*Assignment: organization-defined frequency*], unannounced attempts to bypass or circumvent security controls associated with physical access points to the facility.

Supplemental Guidance: Related controls: CA-2, CA-7.

References: FIPS Publication 201; NIST Special Publications 800-73, 800-76, 800-78, 800-116; ICD 704, 705; DoDI 5200.39; Personal Identity Verification (PIV) in Enterprise Physical Access Control System (E-PACS); Web: idmanagement.gov, fips201ep.cio.gov.

Deleted: Enhancement

Deleted: control

Deleted: ; DCID 6/9

Priority and Baseline Allocation:

P1	**LOW** PE-3	**MOD** PE-3	**HIGH** PE-3 (1)

PE-4 ACCESS CONTROL FOR TRANSMISSION MEDIUM

Control: The organization controls physical access to [*Assignment: organization-defined information system distribution and transmission lines*] within organizational facilities using [*Assignment: organization-defined security safeguards*].

Deleted: .

Supplemental Guidance: Physical security safeguards applied to information system distribution and transmission lines help to prevent accidental damage, disruption, and physical tampering. In addition, physical safeguards may be necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Security safeguards to control physical access to system distribution and transmission lines include, for example: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays. Related controls: MP-2, MP-4, PE-2, PE-3, PE-5, SC-7, SC-8.

Deleted: protections

Deleted: Additionally

Deleted: protections are

Deleted: Protective measures

Deleted: information

Deleted:

Deleted: control:

Control Enhancements: None.

References: NSTISSI No. 7003.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** PE-4	**HIGH** PE-4

PE-5 ACCESS CONTROL FOR OUTPUT DEVICES

Control: The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

Supplemental Guidance: Controlling physical access to output devices includes, for example, placing output devices in locked rooms or other secured areas and allowing access to authorized individuals only, and placing output devices in locations that can be monitored by organizational personnel. Monitors, printers, copiers, scanners, facsimile machines, and audio devices are examples of information system output devices. Related controls: PE-2, PE-3, PE-4, PE-18.

Control Enhancements:

Deleted: None.

(1) *ACCESS CONTROL FOR OUTPUT DEVICES | ACCESS TO OUTPUT BY AUTHORIZED INDIVIDUALS*

The organization:

(a) Controls physical access to output from [*Assignment: organization-defined output devices*]; and

(b) Ensures that only authorized individuals receive output from the device.

Supplemental Guidance: Controlling physical access to selected output devices includes, for example, placing printers, copiers, and facsimile machines in controlled areas with keypad access controls or limiting access to individuals with certain types of badges.

(2) *ACCESS CONTROL FOR OUTPUT DEVICES | ACCESS TO OUTPUT BY INDIVIDUAL IDENTITY*

The information system:

(a) Controls physical access to output from [*Assignment: organization-defined output devices*]; and

(b) Links individual identity to receipt of the output from the device.

Supplemental Guidance: Controlling physical access to selected output devices includes, for example, installing security functionality on printers, copiers, and facsimile machines that allows organizations to implement authentication (e.g., using a PIN or hardware token) on output devices prior to the release of output to individuals.

(3) *ACCESS CONTROL FOR OUTPUT DEVICES | MARKING OUTPUT DEVICES*

The organization marks [*Assignment: organization-defined information system output devices*] indicating the appropriate security marking of the information permitted to be output from the device.

Supplemental Guidance: Outputs devices include, for example, printers, monitors, facsimile machines, scanners, copiers, and audio devices. This control enhancement is generally applicable to information system output devices other than mobiles devices.

References: None.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** PE-5	**HIGH** PE-5

Deleted: P1

PE-6 MONITORING PHYSICAL ACCESS

Control: The organization:

a. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents;

b. Reviews physical access logs [*Assignment: organization-defined frequency*] and upon occurrence of [*Assignment: organization-defined events or potential indications of events*]; and

c. Coordinates results of reviews and investigations with the organizational incident response capability.

Deleted: organization's

Supplemental Guidance: Organizational incident response capabilities include investigations of and responses to detected physical security incidents. Security incidents include, for example, apparent security violations or suspicious physical access activities. Suspicious physical access activities include, for example: (i) accesses outside of normal work hours; (ii) repeated accesses to areas not normally accessed; (iii) accesses for unusual lengths of time; and (iv) out-of-sequence accesses. Related controls: CA-7, IR-4, IR-8.

Deleted: Investigation

Deleted: response

Deleted: , including

Control Enhancements:

(1) *MONITORING PHYSICAL ACCESS | INTRUSION ALARMS / SURVEILLANCE EQUIPMENT*

The organization monitors physical intrusion alarms and surveillance equipment.

Deleted: and

Deleted: .

(2) *MONITORING PHYSICAL ACCESS | AUTOMATED INTRUSION RECOGNITION / RESPONSES*

The organization employs automated mechanisms to recognize [*Assignment: organization-defined classes/types of intrusions*] and initiate [*Assignment: organization-defined response actions*].

Supplemental Guidance: Related control: SI-4.

Deleted: potential

Deleted: designated

Deleted: .

(3) *MONITORING PHYSICAL ACCESS | VIDEO SURVEILLANCE*

The organization employs video surveillance of [*Assignment: organization-defined operational areas*] and retains video recordings for [*Assignment: organization-defined time period*].

Supplemental Guidance: This control enhancement focuses on recording surveillance video for purposes of subsequent review, if circumstances so warrant (e.g., a break-in detected by other means). It does not require monitoring surveillance video although organizations may choose to do so. Note that there may be legal considerations when performing and retaining video surveillance, especially if such surveillance is in a public location.

(4) *MONITORING PHYSICAL ACCESS | MONITORING PHYSICAL ACCESS TO INFORMATION SYSTEMS*

The organization monitors physical access to the information system in addition to the physical access monitoring of the facility as [*Assignment: organization-defined physical spaces containing one or more components of the information system*].

Supplemental Guidance: This control enhancement provides additional monitoring for those areas within facilities where there is a concentration of information system components (e.g., server rooms, media storage areas, communications centers). Related controls: PS-2, PS-3.

References: None.

Priority and Baseline Allocation:

P1	**LOW** PE-6	**MOD** PE-6 (1)	**HIGH** PE-6 (1) (4)

PE-7 VISITOR CONTROL

[Withdrawn: Incorporated into PE-2 and PE-3].

(1)

PE-8 VISITOR ACCESS RECORDS

Control: The organization:

a. Maintains visitor access records to the facility where the information system resides for [*Assignment: organization-defined time period*]; and

b. Reviews visitor access records [*Assignment: organization-defined frequency*].

Supplemental Guidance: Visitor access records include, for example, names and organizations of persons visiting, visitor signatures, forms of identification, dates of access, entry and departure times, purposes of visits, and names and organizations of persons visited. Visitor access records are not required for publicly accessible areas.

Control Enhancements:

(1) *VISITOR ACCESS RECORDS | AUTOMATED RECORDS MAINTENANCE / REVIEW*

The organization employs automated mechanisms to facilitate the maintenance and review of visitor access records.

(2) *VISITOR ACCESS RECORDS | PHYSICAL ACCESS RECORDS*

[Withdrawn: Incorporated into PE-2].

References: None.

Priority and Baseline Allocation:

P3	**LOW** PE-8	**MOD** PE-8	**HIGH** PE-8 (1)

PE-9 POWER EQUIPMENT AND CABLING

Control: The organization protects power equipment and power cabling for the information system from damage and destruction.

Deleted: (2)

Deleted: Control: The organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible.¶
Supplemental Guidance: Individuals (to include organizational employees, contract personnel, and others) with permanent authorization credentials for the facility are not considered visitors.¶
Control Enhancements:¶
**<#>The organization escorts visitors and monitors visitor activity, when required.¶
The organization requires two forms of identification for visitor access to the facility.**

Moved up [5]: References: None.¶
Priority and Baseline Allocation:¶

Deleted: P1 ...

Deleted: (except for those areas within the facility officially designated as publicly accessible);

Deleted: name/organization

Deleted: the person

Deleted: signature of the

Deleted: , form(s)

Deleted: date

Deleted: time of

Deleted: , purpose

Deleted: visit

Deleted: name/organization

Deleted: person

Deleted:

Deleted: The organization maintains a record of all physical access, both visitor and authorized individuals.

Deleted: (2)

Deleted: POWER

Supplemental Guidance: Organizations determine the types of protection necessary for power equipment and cabling employed at different locations both internal and external to organizational facilities and environments of operation. This includes, for example, generators and power cabling outside of buildings, internal cabling and uninterruptable power sources within an office or data center, and power sources for self-contained entities such as vehicles and satellites. Related control: PE-4.

Deleted: ¶

Deleted: This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

Control Enhancements:

(1) *POWER EQUIPMENT AND CABLING | REDUNDANT CABLING*

The organization employs redundant power cabling paths that are physically separated by [*Assignment: organization-defined distance*].

Supplemental Guidance: Physically separate, redundant power cables help to ensure that power continues to flow in the event one of the cables is cut or otherwise damaged.

Deleted: and parallel

Deleted: .

(2) *POWER EQUIPMENT AND CABLING | AUTOMATIC VOLTAGE CONTROLS*

The organization employs automatic voltage controls for [*Assignment: organization-defined critical information system components*].

Deleted: ***list of***

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** PE-9	**HIGH** PE-9

PE-10 EMERGENCY SHUTOFF

Control: The organization:

a. Provides the capability of shutting off power to the information system or individual system components in emergency situations;

b. Places emergency shutoff switches or devices in [*Assignment: organization-defined location by information system or system component*] to facilitate safe and easy access for personnel; and

c. Protects emergency power shutoff capability from unauthorized activation.

Supplemental Guidance: This control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms. Related control: PE-15.

Control Enhancements:

(1) *EMERGENCY SHUTOFF | ACCIDENTAL / UNAUTHORIZED ACTIVATION*

[Withdrawn: Incorporated into PE-10].

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** PE-10	**HIGH** PE-10

PE-11 EMERGENCY POWER

Control: The organization provides a short-term uninterruptible power supply to facilitate [Selection (one or more): *an orderly shutdown of the information system; transition of the information system to long-term alternate power*] in the event of a primary power source loss.

Supplemental Guidance: Related controls: AT-3, CP-2, CP-7 Control Enhancements:

Deleted: This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.¶

(1) *EMERGENCY POWER | LONG-TERM ALTERNATE POWER SUPPLY - MINIMAL OPERATIONAL CAPABILITY*

The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

Supplemental Guidance: This control enhancement can be satisfied, for example, by the use of a secondary commercial power supply or other external power supply. Long-term alternate power supplies for the information system can be either manually or automatically activated.

(2) *EMERGENCY POWER | LONG-TERM ALTERNATE POWER SUPPLY - SELF-CONTAINED*

The organization provides a long-term alternate power supply for the information system that is:

(a) Self-contained;

(b) Not reliant on external power generation; and

(c) Capable of maintaining [*Selection: minimally required operational capability; full operational capability*] in the event of an extended loss of the primary power source.

Supplemental Guidance: This control enhancement can be satisfied, for example, by the use of one or more generators with sufficient capacity to meet the needs of the organization. Long-term alternate power supplies for organizational information systems are either manually or automatically activated.

Deleted: Enhancement

Deleted: the

Deleted: system

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** PE-11	**HIGH** PE-11 (1)

PE-12 EMERGENCY LIGHTING

Control: The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

Supplemental Guidance: This control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms. Related controls: CP-2, CP-7.

Deleted: ,

Deleted: include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the

Deleted: security program. Organizations avoid duplicating actions already covered

Control Enhancements:

(1) *EMERGENCY LIGHTING | ESSENTIAL MISSIONS / BUSINESS FUNCTIONS*

The organization provides emergency lighting for all areas within the facility supporting essential missions and business functions.

References: None.

Priority and Baseline Allocation:

P1	**LOW** PE-12	**MOD** PE-12	**HIGH** PE-12

PE-13 FIRE PROTECTION

Control: The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

Supplemental Guidance: This control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms. Fire suppression and detection devices/systems include, for example, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors.

Deleted: Supplemental Guidance:

Deleted: This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

Control Enhancements:

(1) *FIRE PROTECTION | DETECTION DEVICES / SYSTEMS*

The organization employs fire detection devices/systems for the information system that activate automatically and notify [*Assignment: organization-defined personnel or roles*] and [*Assignment: organization-defined emergency responders*] in the event of a fire.

Deleted: the

Supplemental Guidance: Organizations can identify specific personnel, roles, and emergency responders in the event that individuals on the notification list must have appropriate access authorizations and/or clearances, for example, to obtain access to facilities where classified operations are taking place or where there are information systems containing classified information.

(2) *FIRE PROTECTION | SUPPRESSION DEVICES / SYSTEMS*

The organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation to *Assignment: organization-defined personnel or roles*] and [*Assignment: organization-defined* emergency responders].

Deleted: the

Deleted: .

Supplemental Guidance: Organizations can identify specific personnel, roles, and emergency responders in the event that individuals on the notification list must have appropriate access authorizations and/or clearances, for example, to obtain access to facilities where classified operations are taking place or where there are information systems containing classified information.

(3) *FIRE PROTECTION | AUTOMATIC FIRE SUPPRESSION*

The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.

(4) *FIRE PROTECTION | INSPECTIONS*

The organization ensures that the facility undergoes [*Assignment: organization-defined frequency*] inspections by authorized and qualified inspectors and resolves identified deficiencies within [*Assignment: organization-defined time period*].

Deleted: fire marshal

Deleted: promptly

Deleted: .

References: None.

Priority and Baseline Allocation:

P1	**LOW** PE-13	**MOD** PE-13 (3)	**HIGH** PE-13 (1) (2) (3)

Deleted: 1) (2) (

PE-14 TEMPERATURE AND HUMIDITY CONTROLS

Control: The organization:

a. Maintains temperature and humidity levels within the facility where the information system resides at [*Assignment: organization-defined acceptable levels*]; and

b. Monitors temperature and humidity levels [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control applies primarily to facilities containing concentrations of information system resources, for example, data centers, server rooms, and mainframe computer rooms. Related control: AT-3.

Deleted: ,

Deleted: include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the

Deleted: security program. Organizations avoid duplicating actions already covered

Control Enhancements:

(1) *TEMPERATURE AND HUMIDITY CONTROLS | AUTOMATIC CONTROLS*

The organization employs automatic temperature and humidity controls in the facility to prevent fluctuations potentially harmful to the information system.

(2) *TEMPERATURE AND HUMIDITY CONTROLS | MONITORING WITH ALARMS / NOTIFICATIONS*

The organization employs temperature and humidity monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment.

References: None.

Priority and Baseline Allocation:

P1	**LOW** PE-14	**MOD** PE-14	**HIGH** PE-14

PE-15 WATER DAMAGE PROTECTION

Control: The organization protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

Supplemental Guidance: This control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms. Isolation valves can be employed in addition to or in lieu of master shutoff valves to shut off water supplies in specific areas of concern, without affecting entire organizations. Related control: AT-3.

Deleted: Supplemental Guidance: This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.¶

Control Enhancements:

(1) *WATER DAMAGE PROTECTION | AUTOMATION SUPPORT*

The organization employs automated mechanisms to detect the presence of water in the vicinity of the information system and alerts [*Assignment: organization-defined personnel or roles*].

Supplemental Guidance: Automated mechanisms can include, for example, water detection sensors, alarms, and notification systems.

Deleted: that, without

Deleted: need for manual intervention, protect

Deleted: from water damage in the event of a water leak.

References: None.

Priority and Baseline Allocation:

P1	**LOW** PE-15	**MOD** PE-15	**HIGH** PE-15 (1)

PE-16 DELIVERY AND REMOVAL

Control: The organization authorizes, monitors, and controls [*Assignment: organization-defined types of information system components*] entering and exiting the facility and maintains records of those items.

Supplemental Guidance: Effectively enforcing authorizations for entry and exit of information system components may require restricting access to delivery areas and possibly isolating the areas from the information system and media libraries. Related controls: CM-3, MA-2, MA-3, MP-5, SA-12.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P2	**LOW** PE-16	**MOD** PE-16	**HIGH** PE-16

Deleted: P1

PE-17 ALTERNATE WORK SITE

Control: The organization:

a. Employs [*Assignment: organization-defined security controls*] at alternate work sites;

Deleted: *management, operational, and technical information system*

b. Assesses as feasible, the effectiveness of security controls at alternate work sites; and

c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.

Supplemental Guidance: Alternate work sites may include, for example, government facilities or private residences of employees. While commonly distinct from alternative processing sites, alternate work sites may provide readily available alternate locations as part of contingency operations. Organizations may define different sets of security controls for specific alternate work sites or types of sites depending on the work-related activities conducted at those sites. This control supports the contingency planning activities of organizations and the federal telework initiative. Related controls: AC-17, CP-7.

Deleted: The organization

Control Enhancements: None.

References: NIST Special Publication 800-46.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** PE-17	**HIGH** PE-17

Deleted: P1

PE-18 LOCATION OF INFORMATION SYSTEM COMPONENTS

Control: The organization positions information system components within the facility to minimize potential damage from [*Assignment: organization-defined physical and environmental hazards*] and to minimize the opportunity for unauthorized access.

Supplemental Guidance: Physical and environmental hazards include, for example, flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electromagnetic pulse, electrical interference, and other forms of incoming electromagnetic radiation. In addition, organizations consider the location of physical entry points where unauthorized individuals, while not being granted access, might nonetheless be in close proximity to information systems and therefore increase the potential for unauthorized access to organizational communications (e.g., through the use of wireless sniffers or microphones). Related controls: CP-2, PE-19, RA-3.

Deleted: Whenever possible, the organization also considers the location or site of the facility with regard to physical and environmental hazards.

Deleted: the organization considers

Deleted: the

Deleted: system

Deleted: ,

Deleted: This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered

Control Enhancements:

(1) *LOCATION OF INFORMATION SYSTEM COMPONENTS | FACILITY SITE*

The organization plans the location or site of the facility where the information system resides with regard to physical and environmental hazards and for existing facilities, considers the physical and environmental hazards in its risk mitigation strategy.

Supplemental Guidance: Related control: PM-8.

References: None.

Priority and Baseline Allocation:

P3	**LOW** Not Selected	**MOD** Not Selected	**HIGH** PE-18

Deleted: P2

Deleted: PE-18

Deleted: (1)

PE-19 INFORMATION LEAKAGE

Control: The organization protects the information system from information leakage due to electromagnetic signals emanations.

Supplemental Guidance: Information leakage is the intentional or unintentional release of information to an untrusted environment from electromagnetic signals emanations. Security categories or classifications of information systems (with respect to confidentiality) and organizational security policies guide the selection of security controls employed to protect systems against information leakage due to electromagnetic signals emanations.

Deleted: The security categorization of

Deleted: system

Deleted: policy guides

Deleted: application of safeguards and countermeasures

Deleted: the information system

Control Enhancements:

(1) *INFORMATION LEAKAGE | NATIONAL EMISSIONS / TEMPEST POLICIES AND PROCEDURES*

The organization ensures that information system components, associated data communications, and networks are protected in accordance with national emissions and TEMPEST policies and procedures based on the security category or classification of the information.

References: FIPS Publication 199.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

PE-20 ASSET MONITORING AND TRACKING

Control: The organization:

a. Employs [*Assignment: organization-defined asset location technologies*] to track and monitor the location and movement of [*Assignment: organization-defined assets*] within [*Assignment: organization-defined controlled areas*]; and

b. Ensures that asset location technologies are employed in accordance with applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance.

Supplemental Guidance: Asset location technologies can help organizations ensure that critical assets such as vehicles or essential information system components remain in authorized locations. Organizations consult with the Office of the General Counsel and the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) regarding the deployment and use of asset location technologies to address potential privacy concerns. Related control: CM-8.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

Deleted: : (i)

Deleted: ; and (ii)

Deleted: sensitivity of the

Deleted: being transmitted

FAMILY: PLANNING

PL-1 SECURITY PLANNING POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

1. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the security planning policy and associated security planning controls; and

b. Reviews and updates the current:

1. Security planning policy [*Assignment: organization-defined frequency*]; and

2. Security planning procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PL family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-18, 800-100.

Priority and Baseline Allocation:

P1	**LOW** PL-1	**MOD** PL-1	**HIGH** PL-1

PL-2 SYSTEM SECURITY PLAN

Control: The organization:

a. Develops a security plan for the information system that:

1. Is consistent with the organization’s enterprise architecture;

2. Explicitly defines the authorization boundary for the system;

3. Describes the operational context of the information system in terms of missions and business processes;

4. Provides the security categorization of the information system including supporting rationale;

5. Describes the operational environment for the information system and relationships with or connections to other information systems;

6. Provides an overview of the security requirements for the system;

7. Identifies any relevant overlays, if applicable;

Deleted: develops

Deleted: , and reviews/updates

Deleted: *frequency*

Deleted: A formal, documented

Deleted: Formal, documented procedures

Deleted: .

Deleted: is intended to produce

Deleted: that are required

Deleted: security planning

Deleted: The policy

Deleted: are consistent with

Deleted: policies,

Deleted: Existing organizational

Deleted: additional

Deleted: The security planning policy addresses the overall policy requirements for confidentiality, integrity, and availability and

Deleted: the organization. Security planning

Deleted: developed

Deleted: a

Deleted: system, when required.

Deleted: the development of the security planning

Deleted: .

Deleted: category and impact level

Deleted: <#>Describes relationships with or connections to other information systems;¶

8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and

9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;

b. Distributes copies of the security plan and communicates subsequent changes to the plan to [*Assignment: organization-defined personnel or roles*];

c. Reviews the security plan for the information system [*Assignment: organization-defined frequency*];

d. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and

e. Protects the security plan from unauthorized disclosure and modification.

Supplemental Guidance: Security plans relate security requirements to a set of security controls and control enhancements. Security plans also describe, at a high level, how the security controls and control enhancements meet those security requirements, but do not provide detailed, technical descriptions of the specific design or implementation of the controls/enhancements. Security 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 security control baselines in Appendix D and CNSS Instruction1253 to develop *overlays* for community-wide use or to address specialized requirements, technologies, or missions/environments of operation (e.g., DoD-tactical, Federal Public Key Infrastructure, or Federal Identity, Credential, and Access Management, space operations). Appendix I provides guidance on developing overlays.

Security plans need not be single documents; the plans can be a collection of various documents including documents that already exist. Effective security plans make extensive use of references to policies, procedures, and additional documents (e.g., design and implementation specifications) where more detailed information can be obtained. This reduces the documentation requirements associated with security programs and maintains security-related information in other established management/operational areas related to enterprise architecture, system development life cycle, systems engineering, and acquisition. For example, security plans do not contain detailed contingency plan or incident response plan information but instead provide explicitly or by reference, sufficient information to define what needs to be accomplished by those plans. Related controls: AC-2, AC-6, AC-14, AC-17, AC-20, CA-2, CA-3, CA-7, CM-9, CP-2, IR-8, MA-4, MA-5, MP-2, MP-4, MP-5, PL-7, PM-1, PM-7, PM-8, PM-9, PM-11, SA-5, SA-17.

Control Enhancements:

(1) *SYSTEM SECURITY PLAN | CONCEPT OF OPERATIONS*

[Withdrawn: Incorporated into PL-7].

(2) *SYSTEM SECURITY PLAN | FUNCTIONAL ARCHITECTURE*

[Withdrawn: Incorporated into PL-8].

(3) *SYSTEM SECURITY PLAN | PLAN / COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES*

The organization plans and coordinates security-related activities affecting the information system with [*Assignment: organization-defined individuals or groups*] before conducting such activities in order to reduce the impact on other organizational entities.

Supplemental Guidance: Security-related activities include, for example, security assessments, audits, hardware and software maintenance, patch management, and contingency plan testing. Advance planning and coordination includes emergency and nonemergency (i.e., planned or nonurgent unplanned) situations. The process defined by organizations to plan and coordinate

Deleted: and

Deleted: .

Deleted: The security plan contains

Deleted: parameters

Deleted: in security controls

Deleted: an

Deleted: plan

Deleted: a

Deleted: determination

Deleted: The organization:¶
<#>Develops a security Concept of Operations (CONOPS) for the information system containing, at a minimum: (i) the purpose of the system; (ii) a description of the system architecture; (iii) the security authorization schedule; and (iv) the security categorization and associated factors considered in determining the categorization; and¶
Reviews and updates the CONOPS [*Assignment: organization-defined frequency*].

Deleted: Enhancement Supplemental Guidance: The security CONOPS may be included in the security plan for the information system.

Deleted: The organization develops a functional architecture for the information system that identifies and maintains:¶
<#>External interfaces, the information being exchanged across the interfaces, and the protection mechanisms associated with each interface;¶
<#>User roles and the access privileges assigned to each role;¶
<#>Unique security requirements;¶
<#>Types of information processed, stored, or transmitted by the information system and any specific protection needs in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; and¶
<#>Restoration priority of information or information system services.¶
Enhancement Supplemental Guidance: Unique security requirements for the information system include, for example, encryption of key data elements at rest. Specific protection needs for the information system include, for example, the Privacy Act and Health Insurance Portability and Accountability Act.¶

security-related activities can be included in security plans for information systems or other documents, as appropriate. Related controls: CP-4, IR-4.

References: NIST Special Publication 800-18.

Priority and Baseline Allocation:

P1	**LOW** PL-2	**MOD** PL-2 (3)	**HIGH** PL-2 (3)

PL-3 SYSTEM SECURITY PLAN UPDATE

[Withdrawn: Incorporated into PL-2].

PL-4 RULES OF BEHAVIOR

Control: The organization:

a. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage;

b. Receives a signed 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 information system;

Deleted: all

Deleted: users

Deleted: and

Deleted: users

Deleted: .

c. Reviews and updates the rules of behavior [*Assignment: organization-defined frequency*]; and

d. Requires individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised/updated.

Supplemental Guidance: This control enhancement applies to organizational users. Organizations consider rules of behavior based on individual user roles and responsibilities, differentiating, for example, between rules that apply to privileged users and rules that apply to general users. Establishing rules of behavior for some types of non-organizational users including, for example, individuals who simply receive data/information from federal information 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 both organizational and non-organizational users can also be established in AC-8, System Use Notification. PL-4 b. (the signed acknowledgment portion of this control) may be satisfied by the security awareness training and role-based security training programs conducted by organizations if such training includes rules of behavior. Organizations can use electronic signatures for acknowledging rules of behavior. Related controls: AC-2, AC-6, AC-8, AC-9, AC-17, AC-18, AC-19, AC-20, AT-2, AT-3, CM-11, IA-2, IA-4, IA-5, MP-7, PS-6, PS-8, SA-5.

Deleted: The organization considers different sets of rules

Deleted: for example,

Deleted:

Deleted: the

Deleted: Electronic

Deleted: are acceptable

Deleted: use in

Deleted:

Deleted: control:

Control Enhancements:

(1) *RULES OF BEHAVIOR | SOCIAL MEDIA AND NETWORKING RESTRICTIONS*

The organization includes in the rules of behavior, explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.

Supplemental Guidance: This control enhancement addresses rules of behavior related to the use of social media/networking sites: (i) when organizational personnel are using such sites for official duties or in the conduct of official business; (ii) when organizational information is involved in social media/networking transactions; and (iii) when personnel are accessing social media/networking sites from organizational information systems. Organizations also address specific rules that prevent unauthorized entities from obtaining and/or inferring non-public organizational information (e.g., system account information, personally identifiable information) from social media/networking sites.

Deleted: ,

Deleted: commercial

Deleted: , and sharing information

References: NIST Publication 800-18.

Priority and Baseline Allocation:

P2	**LOW** PL-4	**MOD** PL-4 (1)	**HIGH** PL-4 (1)

PL-5 PRIVACY IMPACT ASSESSMENT

[Withdrawn: Incorporated into Appendix J, AR-2].

PL-6 SECURITY-RELATED ACTIVITY PLANNING

[Withdrawn: Incorporated into PL-2].

PL-7 SECURITY CONCEPT OF OPERATIONS

Control: The organization:

a. Develops a security Concept of Operations (CONOPS) for the information system containing at a minimum, how the organization intends to operate the system from the perspective of information security; and

b. Reviews and updates the CONOPS [*Assignment: organization-defined frequency*].

Supplemental Guidance: The security CONOPS may be included in the security plan for the information system or in other system development life cycle-related documents, as appropriate. Changes to the CONOPS are reflected in ongoing updates to the security plan, the information security architecture, and other appropriate organizational documents (e.g., security specifications for procurements/acquisitions, system development life cycle documents, and systems/security engineering documents). Related control: PL-2.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

PL-8 INFORMATION SECURITY ARCHITECTURE

Control: The organization:

a. Develops an information security architecture for the information system that:

1. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information;

2. Describes how the information security architecture is integrated into and supports the enterprise architecture; and

3. Describes any information security assumptions about, and dependencies on, external services;

b. Reviews and updates the information security architecture [*Assignment: organization-defined frequency*] to reflect updates in the enterprise architecture; and

Deleted: P1

Deleted: Control: The organization conducts a privacy impact assessment on the information system in accordance with OMB policy.¶
Supplemental Guidance: None

Deleted: References: OMB Memorandum 03-22.¶
P1

Deleted: Control: The organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals.

Deleted: Supplemental Guidance: Security-related activities include, for example, security assessments, audits, system hardware and software maintenance, and contingency plan testing/exercises. Organizational advance planning and coordination includes both emergency and nonemergency (i.e., planned or nonurgent unplanned) situations.

Deleted: P3

Deleted: plans and coordinates

c. Ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions.

Supplemental Guidance: This control addresses actions taken by organizations in the design and development of information systems. The information security architecture at the individual information system level is consistent with and complements the more global, organization-wide information security architecture described in PM-7 that is integral to and developed as part of the enterprise architecture. The information security architecture includes an architectural description, the placement/allocation of security functionality (including security controls), security-related information for external interfaces, information being exchanged across the interfaces, and the protection mechanisms associated with each interface. In addition, the security architecture can include other important security-related information, for example, user roles and access privileges assigned to each role, unique security requirements, the types of information processed, stored, and transmitted by the information system, restoration priorities of information and information system services, and any other specific protection needs.

In today's modern architecture, it is becoming less common for organizations to control all information resources. There are going to be key dependencies on external information services and service providers. Describing such dependencies in the information security architecture is important to developing a comprehensive mission/business protection strategy. Establishing, developing, documenting, and maintaining under configuration control, a baseline configuration for organizational information systems is critical to implementing and maintaining an effective information security architecture. The development of the information security architecture is coordinated with the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) to ensure that security controls needed to support privacy requirements are identified and effectively implemented. PL-8 is primarily directed at organizations (i.e., internally focused) to help ensure that organizations develop an information security architecture for the information system, and that the security architecture is integrated with or tightly coupled to the enterprise architecture through the organization-wide information security architecture. In contrast, SA-17 is primarily directed at external information technology product/system developers and integrators (although SA-17 could be used internally within organizations for in-house system development). SA-17, which is complementary to PL-8, is selected when organizations outsource the development of information systems or information system components to external entities, and there is a need to demonstrate/show consistency with the organization's enterprise architecture and information security architecture. Related controls: CM-2, CM-6, PL-2, PM-7, SA-5, SA-17, Appendix J.

Control Enhancements:

(1) *INFORMATION SECURITY ARCHITECTURE | DEFENSE-IN-DEPTH*

The organization designs its security architecture using a defense-in-depth approach that:

(a) Allocates [*Assignment: organization-defined security safeguards*] to [*Assignment: organization-defined locations and architectural layers*]; and

(b) Ensures that the allocated security safeguards operate in a coordinated and mutually reinforcing manner.

Supplemental Guidance: Organizations strategically allocate security safeguards (procedural, technical, or both) in the security architecture so that adversaries have to overcome multiple safeguards to achieve their objective. Requiring adversaries to defeat multiple mechanisms makes it more difficult to successfully attack critical information resources (i.e., increases adversary work factor) and also increases the likelihood of detection. The coordination of allocated safeguards is essential to ensure that an attack that involves one safeguard does not create adverse unintended consequences (e.g., lockout, cascading alarms) by interfering with another safeguard. Placement of security safeguards is a key activity. Greater asset criticality or information value merits additional layering. Thus, an organization may choose to place anti-virus software at organizational boundary layers, email/web servers, notebook computers, and workstations to maximize the number of related safeguards adversaries must penetrate before compromising the information and information systems. Related controls: SC-29, SC-36.

(2) *INFORMATION SECURITY ARCHITECTURE | SUPPLIER DIVERSITY*

The organization requires that [*Assignment: organization-defined security safeguards*] allocated to [*Assignment: organization-defined locations and architectural layers*] are obtained from different suppliers.

Supplemental Guidance: Different information technology products have different strengths and weaknesses. Providing a broad spectrum of products complements the individual offerings. For example, vendors offering malicious code protection typically update their products at different times, often developing solutions for known viruses, Trojans, or worms according to their priorities and development schedules. By having different products at different locations (e.g., server, boundary, desktop) there is an increased likelihood that at least one will detect the malicious code. Related control: SA-12.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** PL-8	**HIGH** PL-8

PL-9 CENTRAL MANAGEMENT

Control: The organization centrally manages [*Assignment: organization-defined security controls and related processes*].

Supplemental Guidance: Central management refers to the organization-wide management and implementation of selected security controls and related processes. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed security controls and processes. As central management of security controls is generally associated with common controls, such management promotes and facilitates standardization of security control implementations and management and judicious use of organizational resources. Centrally-managed security controls and processes may also meet independence requirements for assessments in support of initial and ongoing authorizations to operate as part of organizational continuous monitoring. As part of the security control selection process, organizations determine which controls may be suitable for central management based on organizational resources and capabilities. Organizations consider that it may not always be possible to centrally manage every aspect of a security control. In such cases, the security control is treated as a hybrid control with the control managed and implemented either centrally or at the information system level. 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) (6) (8) (9); AC-22; AC-23; AT-2 (1) (2); AT-3 (1) (2) (3); AT-4; AT-5; 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 Publication 800-37.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

FAMILY: PERSONNEL SECURITY

PS-1 PERSONNEL SECURITY POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

1. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls; and

b. Reviews and updates the current:

1. Personnel security policy [*Assignment: organization-defined frequency*]; and

2. Personnel security procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PS family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

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

Priority and Baseline Allocation:

P1	**LOW** PS-1	**MOD** PS-1	**HIGH** PS-1

PS-2 POSITION RISK DESIGNATION

Control: The organization:

a. Assigns a risk designation to all organizational positions;

b. Establishes screening criteria for individuals filling those positions; and

c. Reviews and updates position risk designations [*Assignment: organization-defined frequency*].

Supplemental Guidance: Position risk designations reflect Office of Personnel Management policy and guidance. Risk designations can guide and inform the types of authorizations individuals receive when accessing organizational information and information systems. Position screening criteria include explicit information security role appointment requirements (e.g., training, security clearances). Related controls: AT-3, PL-2, PS-3.

Control Enhancements: None.

References: 5 C.F.R. 731.106(a).

Priority and Baseline Allocation:

Deleted:
CLASS: OPERATIONAL

Deleted: develops,

Deleted: , and reviews/updates

Deleted: *frequency*

Deleted: A formal, documented

Deleted: Formal, documented procedures

Deleted: .

Deleted: is intended to produce

Deleted: that are required

Deleted: personnel security

Deleted: The policy

Deleted: are consistent with

Deleted: policies,

Deleted: Existing organizational

Deleted: additional

Deleted:

Deleted: personnel security

Deleted: the organization. Personnel security

Deleted: developed

Deleted: a

Deleted: system, when required.

Deleted: the development of the personnel security

Deleted: .

Deleted: CATEGORIZATION

Deleted: revises

Deleted: are consistent with

Deleted: The

Deleted: clearance).

Deleted: CFR

P1	**LOW** PS-2	**MOD** PS-2	**HIGH** PS-2

PS-3 PERSONNEL SCREENING

Control: The organization:

a. Screens individuals prior to authorizing access to the information system; and

b. Rescreens individuals according to [*Assignment: organization-defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of such rescreening*].

Deleted: *list of*

Deleted: *re-screening*

Supplemental Guidance: Personnel screening and rescreening activities reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, guidance, and specific criteria established for the risk designations of assigned positions. Organizations may define different rescreening conditions and frequencies for personnel accessing information systems based on types of information processed, stored, or transmitted by the systems. Related controls: AC-2, IA-4, PE-2, PS-2.

Deleted: Screening

Deleted: are consistent with

Deleted: policies,

Deleted: the

Deleted: designation

Deleted: the

Deleted: position. The organization

Deleted: the

Deleted: system

Deleted: the type

Deleted: system

Control Enhancements:

(1) *PERSONNEL SCREENING | CLASSIFIED INFORMATION*

The organization ensures that individuals accessing an information system processing, storing, or transmitting classified information are cleared and indoctrinated to the highest classification level of the information to which they have access on the system.

Supplemental Guidance: Related controls: AC-3, AC-4.

Deleted: every user

Deleted: is

(2) *PERSONNEL SCREENING | FORMAL INDOCTRINATION*

The organization ensures that individuals accessing an information system processing, storing, or transmitting types of classified information which require formal indoctrination, are formally indoctrinated for all of the relevant types of information to which they have access on the system.

Supplemental Guidance: Types of classified information requiring formal indoctrination include, for example, Special Access Program (SAP), Restricted Data (RD), and Sensitive Compartment Information (SCI). Related controls: AC-3, AC-4.

Deleted: every user

Deleted: is

Deleted: Enhancement

(3) *PERSONNEL SCREENING | INFORMATION WITH SPECIAL PROTECTION MEASURES*

The organization ensures that individuals accessing an information system processing, storing, or transmitting information requiring special protection:

(a) Have valid access authorizations that are demonstrated by assigned official government duties; and

(b) Satisfy [*Assignment: organization-defined additional personnel screening criteria*].

Supplemental Guidance: Organizational information requiring special protection includes, for example, Controlled Unclassified Information (CUI) and Sources and Methods Information (SAMI). Personnel security criteria include, for example, position sensitivity background screening requirements.

Moved (insertion) [11]

References: 5 C.F.R. 731.106; FIPS Publications 199, 201; NIST Special Publications 800-60, 800-73, 800-76, 800-78; ICD 704.

Deleted: CFR

Priority and Baseline Allocation:

P1	**LOW** PS-3	**MOD** PS-3	**HIGH** PS-3

PS-4 PERSONNEL TERMINATION

Control: The organization, upon termination of individual employment:

a. Disables information system access within [*Assignment: organization-defined time period*];

Deleted: Terminates

b. Terminates/revokes any authenticators/credentials associated with the individual;

c. Conducts exit interviews that include a discussion of [*Assignment: organization-defined information security topics*];

d. Retrieves all security-related organizational information system-related property;

e. Retains access to organizational information and information systems formerly controlled by terminated individual; and

f. Notifies [*Assignment: organization-defined personnel or roles*] within [*Assignment: organization-defined time period*].

Supplemental Guidance: Information 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 information 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 nonavailability 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 information system accounts of individuals that are being terminated prior to the individuals being notified. Related controls: AC-2, IA-4, PE-2, PS-5, PS-6.

Control Enhancements:

(1) *PERSONNEL TERMINATION | POST-EMPLOYMENT REQUIREMENTS*

The organization:

(a) Notifies terminated individuals of applicable, legally binding post-employment requirements for the protection of organizational information; and

(b) Requires terminated individuals to sign an acknowledgment of post-employment requirements as part of the organizational termination process.

Supplemental Guidance: Organizations consult with the Office of the General Counsel regarding matters of post-employment requirements on terminated individuals.

(2) *PERSONNEL TERMINATION | AUTOMATED NOTIFICATION*

The organization employs automated mechanisms to notify [*Assignment: organization-defined personnel or roles*] upon termination of an individual.

Supplemental Guidance: In organizations with a large number of employees, not all personnel who need to know about termination actions receive the appropriate notifications—or, if such notifications are received, they may not occur in a timely manner. Automated mechanisms can be used to send automatic alerts or notifications to specific organizational personnel or roles (e.g., management personnel, supervisors, personnel security officers, information security officers, systems administrators, or information technology administrators) when individuals are terminated. Such automatic alerts or notifications can be conveyed in a variety of ways, including, for example, telephonically, via electronic mail, via text message, or via websites.

References: None.

Priority and Baseline Allocation:

P1	**LOW** PS-4	**MOD** PS-4	**HIGH** PS-4 (2)

PS-5 PERSONNEL TRANSFER

Control: The organization:

Deleted: ;

Deleted: and

Deleted: .

Deleted:

Deleted: any

Deleted: all

Deleted: employees (e.g.,

Deleted: the case of

Deleted: some

Deleted:).

Deleted:

Deleted: this control

Deleted: particularly

Deleted: employees or contractors

Deleted: reviews

a. Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization;

b. Initiates [*Assignment: organization-defined transfer or reassignment actions*] within [*Assignment: organization-defined time period following the formal transfer action*];

c. Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and

d. Notifies [*Assignment: organization-defined personnel or roles*] within [*Assignment: organization-defined time period*].

Supplemental Guidance: This control applies when reassignments or transfers of individuals are permanent or of such extended durations as to make the actions warranted. Organizations define actions appropriate for the types of reassignments or transfers, whether permanent or extended. Actions that may be required for personnel transfers or reassignments to other positions within organizations include, for example: (i) returning old and issuing new keys, identification cards, and building passes; (ii) closing information system accounts and establishing new accounts; (iii) changing information system access authorizations (i.e., privileges); and (iv) providing for access to official records to which individuals had access at previous work locations and in previous information system accounts. Related controls: AC-2, IA-4, PE-2, PS-4.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P2	**LOW** PS-5	**MOD** PS-5	**HIGH** PS-5

PS-6 ACCESS AGREEMENTS

Control: The organization:

a. Develops and documents access agreements for organizational information systems;

b. Reviews and updates the access agreements [*Assignment: organization-defined frequency*]; and

c. Ensures that individuals requiring access to organizational information and information systems:

1. Sign appropriate access agreements prior to being granted access; and

2. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or [*Assignment: organization-defined frequency*].

Supplemental Guidance: Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Signed access agreements include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with organizational information systems to which access is authorized. Organizations can use electronic signatures to acknowledge access agreements unless specifically prohibited by organizational policy. Related control: PL-4, PS-2, PS-3, PS-4, PS-8.

Control Enhancements:

(1) *ACCESS AGREEMENTS | INFORMATION REQUIRING SPECIAL PROTECTION*

[Withdrawn: Incorporated into PS-3].

Deleted: personnel

Deleted: and initiates

Deleted:].

Deleted: the reassignment

Deleted: transfer

Deleted: an employee is

Deleted: an

Deleted: duration

Deleted: In addition the organization defines the

Deleted: type

Deleted: reassignment

Deleted: transfer;

Deleted: temporary.

Deleted: when

Deleted: are transferred

Deleted: reassigned

Deleted: the organization

Deleted: previous

Deleted: ;

Deleted: the employee

Deleted: the

Deleted: location

Deleted: the

Deleted: sign

Deleted: Reviews/updates the

Deleted:

Deleted: the

Deleted: system

Deleted: Electronic

Deleted: are acceptable for use in acknowledging

Deleted:

Deleted: The organization ensures that access to

Deleted: information with

Deleted: special protection measures is granted only to individuals who:

Deleted: Have a valid

Deleted: <#>Access authorization that is demonstrated by assigned official government duties; and¶
<#>Satisfy associated personnel security criteria.¶ …

Deleted: measures includes, for example, …

Moved up [11]: Personnel security criteria …

(2) *ACCESS AGREEMENTS | CLASSIFIED INFORMATION REQUIRING SPECIAL PROTECTION*

The organization ensures that access to classified information requiring special protection is granted only to individuals who:

(a) Have a valid access authorization that is demonstrated by assigned official government duties;

(b) Satisfy associated personnel security criteria; and

(c) Have read, understood, and signed a nondisclosure agreement.

Supplemental Guidance: Classified information requiring special protection includes, for example, collateral information, Special Access Program (SAP) information, and Sensitive Compartmented Information (SCI). Personnel security criteria reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance.

Deleted: with

Deleted: measures

Deleted: consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance

Deleted: understand

Deleted: Examples of

Deleted: measures include

(3) *ACCESS AGREEMENTS | POST-EMPLOYMENT REQUIREMENTS*

The organization:

(a) Notifies individuals of applicable, legally binding post-employment requirements for protection of organizational information; and

(b) Requires individuals to sign an acknowledgment of these requirements, if applicable, as part of granting initial access to covered information.

Supplemental Guidance: Organizations consult with the Office of the General Counsel regarding matters of post-employment requirements on terminated individuals.

References: None.

Priority and Baseline Allocation:

P3	**LOW** PS-6	**MOD** PS-6	**HIGH** PS-6

PS-7 THIRD-PARTY PERSONNEL SECURITY

Control: The organization:

a. Establishes personnel security requirements including security roles and responsibilities for third-party providers;

b. Requires third-party providers to comply with personnel security policies and procedures established by the organization;

c. Documents personnel security requirements;

d. Requires third-party providers to notify [*Assignment: organization-defined personnel or roles*] of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within [*Assignment: organization-defined time period*]; and

e. Monitors provider compliance.

Supplemental Guidance: Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management. Organizations explicitly include personnel security requirements in acquisition-related documents. Third-party providers may have personnel working at organizational facilities with credentials, badges, or information system privileges issued by organizations. Notifications of third-party personnel changes ensure appropriate termination of privileges and credentials. Organizations define the transfers and terminations deemed reportable by security-related characteristics that include, for example, functions, roles, and nature of credentials/privileges associated with individuals transferred or terminated. Related controls: PS-2, PS-3, PS-4, PS-5, PS-6, SA-9, SA-21.

Deleted: The organization explicitly includes personnel security requirements in acquisition-related documents

Control Enhancements: None.

References: NIST Special Publication 800-35.

Priority and Baseline Allocation:

P1	**LOW** PS-7	**MOD** PS-7	**HIGH** PS-7

PS-8 PERSONNEL SANCTIONS

Control: The organization:

a. Employs a formal sanctions process for individuals failing to comply with established information security policies and procedures; and

b. Notifies [*Assignment: organization-defined personnel or roles*] within [*Assignment: organization-defined time period*] when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

Supplemental Guidance: Organizational sanctions processes reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Sanctions processes are described in access agreements and can be included as part of general personnel policies and procedures for organizations. Organizations consult with the Office of the General Counsel regarding matters of employee sanctions. Related controls: PL-4, PS-6.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P3	**LOW** PS-8	**MOD** PS-8	**HIGH** PS-8

Deleted: employs

Deleted: personnel

Deleted: .

Deleted: The

Deleted: process is consistent with

Deleted: policies,

Deleted: The process is

Deleted: the

Deleted: the organization.

FAMILY: RISK ASSESSMENT

RA-1 RISK ASSESSMENT POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and

b. Reviews and updates the current:

1. Risk assessment policy [*Assignment: organization-defined frequency*]; and

2. Risk assessment procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the RA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

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

Priority and Baseline Allocation:

P1	**LOW** RA-1	**MOD** RA-1	**HIGH** RA-1

RA-2 SECURITY CATEGORIZATION

Control: The organization:

a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;

b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and

c. Ensures that the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.

Supplemental Guidance: Clearly defined authorization boundaries are a prerequisite for effective security categorization decisions. Security categories describe the potential adverse impacts to organizational operations, organizational assets, and individuals if organizational information and information systems are comprised through a loss of confidentiality, integrity, or availability. Organizations conduct the security categorization process as an organization-wide activity with the involvement of chief information officers, senior information security officers, information system owners, mission/business owners, and information owners/stewards. Organizations also

Deleted:
CLASS: MANAGEMENT

Deleted: develops,

Deleted: , and reviews/updates

Deleted: *frequency*

Deleted: A formal, documented

Deleted: Formal, documented procedures

Deleted: .

Deleted: is intended to produce

Deleted: that are required

Deleted: risk assessment

Deleted: The policy

Deleted: are consistent with

Deleted: policies,

Deleted: Existing organizational

Deleted: additional

Deleted:

Deleted: risk assessment

Deleted: the organization. Risk assessment

Deleted: developed

Deleted: a

Deleted: system, when required.

Deleted: the development of the risk assessment

Deleted: .

Deleted: A clearly

Deleted: boundary is

Deleted: an

Deleted: .

Deleted: categorization describes

Deleted: should the

Deleted: system be

Deleted: The organization conducts

Deleted: the

Deleted: officer

Deleted: officer

Deleted: owner

Deleted: The organization

consider the potential adverse impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level adverse impacts. Security categorization processes carried out by organizations facilitate the development of inventories of information assets, and along with CM-8, mappings to specific information system components where information is processed, stored, or transmitted. Related controls: CM-8, MP-4, RA-3, SC-7.

Control Enhancements: None.

References: FIPS Publication 199; NIST Special Publications 800-30, 800-39, 800-60.

Priority and Baseline Allocation:

P1	**LOW** RA-2	**MOD** RA-2	**HIGH** RA-2

RA-3 RISK ASSESSMENT

Control: The organization:

a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;

b. Documents risk assessment results in [*Selection: security plan; risk assessment report;* [*Assignment: organization-defined document*]];

c. Reviews risk assessment results [*Assignment: organization-defined frequency*];

d. Disseminates risk assessment results to [*Assignment: organization-defined personnel or roles*]; and

e. Updates the risk assessment [*Assignment: organization-defined frequency*] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

Supplemental Guidance: Clearly defined authorization boundaries are a prerequisite for effective risk assessments. Risk assessments take into account threats, vulnerabilities, likelihood, and impact to organizational operations and assets, individuals, other organizations, and the Nation based on the operation and use of information systems. Risk assessments also take into account risk from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing organizational information systems, outsourcing entities). In accordance with OMB policy and related E-authentication initiatives, authentication of public users accessing federal information systems may also be required to protect nonpublic or privacy-related information. As such, organizational assessments of risk also address public access to federal information systems.

Risk assessments (either formal or informal) can be conducted at all three tiers in the risk management hierarchy (i.e., organization level, mission/business process level, or information 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, security control selection, security control implementation, security control assessment, information system authorization, and security control monitoring. RA-3 is noteworthy in that the control must be partially implemented prior to the implementation of other controls in order to complete the first two steps in the Risk Management Framework. Risk assessments can play an important role in security control selection processes, particularly during the application of tailoring guidance, which includes security control supplementation. Related controls: RA-2, PM-9.

Control Enhancements: None.

Deleted: considers

Deleted: in categorizing the information system. The security

Deleted: process facilitates the creation

Deleted: an *inventory*

Deleted: in conjunction

Deleted: a mapping

Deleted: the

Deleted: the

Deleted: and

Deleted:

Deleted: and

Deleted: A clearly

Deleted: boundary is

Deleted: an

Deleted: assessment.

Deleted: threat sources, and security controls planned or in place to determine the level of residual risk posed

Deleted: the

Deleted: system.

Deleted: posed to organizational operations, organizational assets, or individuals

Deleted:

Deleted:

Deleted: public access to federal information systems. The General Services Administration provides tools supporting that portion of the risk assessment dealing with

Deleted: by organizations

Deleted: : information system

Deleted: ;

Deleted: ;

Deleted: ;

Deleted: ;

Deleted: ;

Deleted:

Deleted: a

Deleted: security control

Deleted:

Deleted: the

Deleted: process

Deleted: for

Deleted: baselines and when considering supplementing the tailored baselines with ...

Deleted: or control enhancements

References: OMB Memorandum 04-04; NIST Special Publication 800-30, 800-39; Web: idmanagement.gov.

Priority and Baseline Allocation:

P1	**LOW** RA-3	**MOD** RA-3	**HIGH** RA-3

RA-4 RISK ASSESSMENT UPDATE

[Withdrawn: Incorporated into RA-3].

RA-5 VULNERABILITY SCANNING

Control: The organization:

a. Scans for vulnerabilities in the information system and hosted applications [*Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process*] and when new vulnerabilities potentially affecting the system/applications are identified and reported;

b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:

1. Enumerating platforms, software flaws, and improper configurations;
2. Formatting checklists and test procedures; and
3. Measuring vulnerability impact;

c. Analyzes vulnerability scan reports and results from security control assessments;

d. Remediates legitimate vulnerabilities [*Assignment: organization-defined response times*] in accordance with an organizational assessment of risk; and

e. Shares information obtained from the vulnerability scanning process and security control assessments with [*Assignment: organization-defined personnel or roles*] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

Supplemental Guidance: Security categorization of information systems guides the frequency and comprehensiveness of vulnerability scans. Organizations determine the required vulnerability scanning for all information system components, ensuring that potential sources of vulnerabilities such as networked printers, scanners, and copiers are not overlooked. Vulnerability analyses for custom software applications may require additional approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Organizations can employ these analysis approaches in a variety of tools (e.g., web-based application scanners, static analysis tools, binary analyzers) and in source code reviews. Vulnerability scanning includes, for example: (i) scanning for patch levels; (ii) scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and (iii) scanning for improperly configured or incorrectly operating information flow control mechanisms. Organizations consider using tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that use the Open Vulnerability Assessment Language (OVAL) to determine/test for the presence of vulnerabilities. Suggested sources for vulnerability information include the Common Weakness Enumeration (CWE) listing and the National Vulnerability Database (NVD). In addition, security control assessments such as red team exercises provide other sources of potential vulnerabilities for which to scan. Organizations also consider using tools that express vulnerability impact by the Common Vulnerability Scoring System (CVSS). Related controls: CA-2, CA-7, CM-4, CM-6, RA-2, RA-3, SA-11, SI-2.

Deleted: promote

Deleted: and making transparent,

Deleted: designated personnel throughout the

Deleted: The security

Deleted: the

Deleted: system

Deleted: the

Deleted: analysis

Deleted: and

Deleted: , more specialized techniques and

Deleted: , source code analyzers).

Deleted: specific

Deleted: The organization considers

Deleted: The

Deleted:) are also excellent sources for vulnerability information.

Deleted: are another source

Control Enhancements:

(1) *VULNERABILITY SCANNING | UPDATE TOOL CAPABILITY*

The organization employs vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned.

Supplemental Guidance: The vulnerabilities to be scanned need to be readily updated as new vulnerabilities are discovered, announced, and scanning methods developed. This updating process helps to ensure that potential vulnerabilities in the information system are identified and addressed as quickly as possible. Related controls: SI-3, SI-7.

(2) *VULNERABILITY SCANNING | UPDATE BY FREQUENCY / PRIOR TO NEW SCAN / WHEN IDENTIFIED*

The organization updates the information system vulnerabilities scanned *[Selection (one or more):* [*Assignment: organization-defined frequency*]*; prior to a new scan; when new vulnerabilities are identified and reported*].

Supplemental Guidance: Related controls: SI-3, SI-5.

(3) *VULNERABILITY SCANNING | BREADTH / DEPTH OF COVERAGE*

The organization employs vulnerability scanning procedures that can identify the breadth and depth of coverage (i.e., information system components scanned and vulnerabilities checked).

(4) *VULNERABILITY SCANNING | DISCOVERABLE INFORMATION*

The organization determines what information about the information system is discoverable by adversaries and subsequently takes [*Assignment: organization-defined corrective actions*].

Supplemental Guidance: Discoverable information includes information that adversaries could obtain without directly compromising or breaching the information 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 information system to make designated information less relevant or attractive to adversaries. Related control: AU-13.

(5) *VULNERABILITY SCANNING | PRIVILEGED ACCESS*

The information system implements privileged access authorization to [*Assignment: organization-identified information system components*] for selected [*Assignment: organization-defined vulnerability scanning activities*].

Supplemental Guidance: In certain situations, the nature of the vulnerability scanning may be more intrusive or the information system component that is the subject of the scanning may contain highly sensitive information. Privileged access authorization to selected system components facilitates more thorough vulnerability scanning and also protects the sensitive nature of such scanning.

(6) *VULNERABILITY SCANNING | AUTOMATED TREND ANALYSES*

The organization employs automated mechanisms to compare the results of vulnerability scans over time to determine trends in information system vulnerabilities.

Supplemental Guidance: Related controls: IR-4, IR-5, SI-4.

(7) *VULNERABILITY SCANNING | AUTOMATED DETECTION AND NOTIFICATION OF UNAUTHORIZED COMPONENTS*

[Withdrawn: Incorporated into CM-8].

(8) *VULNERABILITY SCANNING | REVIEW HISTORIC AUDIT LOGS*

The organization reviews historic audit logs to determine if a vulnerability identified in the information system has been previously exploited.

Supplemental Guidance: Related control: AU-6.

(9) *VULNERABILITY SCANNING | PENETRATION TESTING AND ANALYSES*

[Withdrawn: Incorporated into CA-8].

(a)

(10) *VULNERABILITY SCANNING | CORRELATE SCANNING INFORMATION*

The organization correlates the output from vulnerability scanning tools to determine the presence of multi-vulnerability/multi-hop attack vectors.

Deleted: list of

Deleted: list of

Deleted:] or

Deleted: .

Deleted: demonstrate

Deleted: attempts to discern

Deleted: .

Deleted: organization includes

Deleted: to facilitate

Deleted: scanning.

Deleted: <#>The organization employs automated mechanisms [*Assignment: organization-defined frequency*] to detect the presence of unauthorized software on organizational information systems and notify designated organizational officials.¶

**Deleted: <#>The organization employs an independent penetration agent or penetration team to:¶
Conduct a**

**Deleted: <#>The organization employs an independent penetration agent or penetration team to:¶
<#>Conduct a vulnerability analysis on the information system; and¶
Perform penetration testing on the information system based on the vulnerability analysis to determine the exploitability of identified vulnerabilities.**

Deleted: <#>Enhancement Supplemental Guidance: A standard method for penetration testing includes: (i) pre-test analysis based on full knowledge of the target information system; (ii) pre-test identification of potential vulnerabilities based on pre-test analysis; and (iii) testing designed to determine exploitability of identified vulnerabilities. Detailed rules of engagement are agreed upon by all parties before the commencement of any penetration testing scenario.¶

References: NIST Special Publications 800-40, 800-70, 800-115; Web: cwe.mitre.org nvd.nist.gov.

Deleted: ;

Priority and Baseline Allocation:

P1	**LOW** RA-5	**MOD** RA-5 (1) (2) (5)	**HIGH** RA-5 (1) (2) (4) (5)

Deleted: 3) (

Deleted: (7)

RA-6 TECHNICAL SURVEILLANCE COUNTERMEASURES SURVEY

Control: The organization employs a technical surveillance countermeasures survey at [*Assignment: organization-defined locations*] [*Selection (one or more)*: [*Assignment: organization-defined frequency*]; [*Assignment: organization-defined events or indicators occur*]].

Supplemental Guidance: Technical surveillance countermeasures surveys are performed by qualified personnel to detect the presence of technical surveillance devices/hazards and to identify technical security weaknesses that could aid in the conduct of technical penetrations of surveyed facilities. Such surveys provide evaluations of the technical security postures of organizations and facilities and typically include thorough visual, electronic, and physical examinations in and about surveyed facilities. The surveys also provide useful input into risk assessments and organizational exposure to potential adversaries.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

FAMILY: SYSTEM AND SERVICES ACQUISITION

SA-1 SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

1. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and

b. Reviews and updates the current:

1. System and services acquisition policy [*Assignment: organization-defined frequency*]; and

2. System and services acquisition procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the SA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

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

Priority and Baseline Allocation:

P1	**LOW** SA-1	**MOD** SA-1	**HIGH** SA-1

SA-2 ALLOCATION OF RESOURCES

Control: The organization:

a. Determines information security requirements for the information system or information system service in mission/business process planning;

b. Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process; and

c. Establishes a discrete line item for information security in organizational programming and budgeting documentation.

Supplemental Guidance: Resource allocation for information security includes funding for the initial information system or information system service acquisition and funding for the sustainment of the system/service. Related controls: PM-3, PM-11.

Control Enhancements: None.

Deleted: **CLASS:** MANAGEMENT

Deleted: develops,

Deleted: , and reviews/updates

Deleted: *frequency*

Deleted: A formal, documented

Deleted: includes information security considerations and that

Deleted: Formal, documented procedures

Deleted: .

Deleted: is intended to produce

Deleted: that are required

Deleted: system and services acquisition

Deleted: The policy

Deleted: are consistent with

Deleted: policies,

Deleted: Existing organizational

Deleted: additional

Deleted:

Deleted: system and services acquisition

Deleted: the organization. System and services acquisition

Deleted: developed

Deleted: a

Deleted: system, when required.

Deleted: the development of the system and services acquisition

Deleted: .

Deleted: Includes a determination of

Deleted: Supplemental Guidance:

References: NIST Special Publication 800-65.

Priority and Baseline Allocation:

P1	**LOW** SA-2	**MOD** SA-2	**HIGH** SA-2

SA-3 SYSTEM DEVELOPMENT LIFE CYCLE

Deleted: SUPPORT

Control: The organization:

a. Manages the information system using [*Assignment: organization-defined system development life cycle*] that incorporates information security considerations;

b. Defines and documents information security roles and responsibilities throughout the system development life cycle;

c. Identifies individuals having information security roles and responsibilities; and

d. Integrates the organizational information security risk management process into system development life cycle activities.

Deleted: a

Deleted: methodology

Deleted: includes

Deleted: system

Deleted: and

Deleted: system

Deleted: .

Deleted: Supplemental Guidance: Related control: PM-7.¶

Supplemental Guidance: A well-defined system development life cycle provides the foundation for the successful development, implementation, and operation of organizational information systems. To apply the required security controls within the system development life cycle requires a basic understanding of information security, threats, vulnerabilities, adverse impacts, and risk to critical missions/business functions. The security engineering principles in SA-8 cannot be properly applied if individuals that design, code, and test information systems and system components (including information technology products) do not understand security. Therefore, organizations include qualified personnel, for example, chief information security officers, security architects, security engineers, and information system security officers in system development life cycle activities to ensure that security requirements are incorporated into organizational information systems. It is equally important that developers include individuals on the development team that possess the requisite security expertise and skills to ensure that needed security capabilities are effectively integrated into the information system. Security awareness and training programs can help ensure that individuals having key security roles and responsibilities have the appropriate experience, skills, and expertise to conduct assigned system development life cycle activities. The effective integration of security requirements into enterprise architecture also helps to ensure that important security considerations are addressed early in the system development life cycle and that those considerations are directly related to the organizational mission/business processes. This process also facilitates the integration of the information security architecture into the enterprise architecture, consistent with organizational risk management and information security strategies. Related controls: AT-3, PM-7, SA-8.

Control Enhancements: None.

References: NIST Special Publications 800-37, 800-64.

Deleted: Publication

Priority and Baseline Allocation:

P1	**LOW** SA-3	**MOD** SA-3	**HIGH** SA-3

SA-4 ACQUISITION PROCESS

Deleted: ACQUISITIONS

Control: The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:

Deleted: /or specifications

Deleted: acquisition contracts based on an assessment of risk and

Deleted: and

a. Security functional requirements;

b. Security strength requirements;

c. Security assurance requirements;

d. Security-related documentation requirements;

e. Requirements for protecting security-related documentation;

f. Description of the information system development environment and environment in which the system is intended to operate; and

g. Acceptance criteria.

Supplemental Guidance: Information system components are discrete, identifiable information technology assets (e.g., hardware, software, or firmware) that represent the building blocks of an information system. Information system components include commercial information technology products. Security functional requirements include security capabilities, security functions, and security mechanisms. Security strength requirements associated with such capabilities, functions, and mechanisms include degree of correctness, completeness, resistance to direct attack, and resistance to tampering or bypass. Security assurance requirements include: (i) development processes, procedures, practices, and methodologies; and (ii) evidence from development and assessment activities providing grounds for confidence that the required security functionality has been implemented and the required security strength has been achieved. Security documentation requirements address all phases of the system development life cycle.

Security functionality, assurance, and documentation requirements are expressed in terms of security controls and control enhancements that have been selected through the tailoring process. The security control tailoring process includes, for example, the specification of parameter values through the use of assignment and selection statements and the specification of platform dependencies and implementation information. Security documentation provides user and administrator guidance regarding the implementation and operation of security controls. The level of detail required in security documentation is based on the security category or classification level of the information system and the degree to which organizations depend on the stated security capability, functions, or mechanisms to meet overall risk response expectations (as defined in the organizational risk management strategy). Security requirements can also include organizationally mandated configuration settings specifying allowed functions, ports, protocols, and services. Acceptance criteria for information systems, information system components, and information system services are defined in the same manner as such criteria for any organizational acquisition or procurement. The Federal Acquisition Regulation (FAR) Section 7.103 contains information security requirements from FISMA. Related controls: CM-6, PL-2, PS-7, SA-3, SA-5, SA-8, SA-11, SA-12.

Control Enhancements:

(1) *ACQUISITION PROCESS | FUNCTIONAL PROPERTIES OF SECURITY CONTROLS*

The organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.

Supplemental Guidance: Functional properties of security controls describe the functionality (i.e., security capability, functions, or mechanisms) visible at the interfaces of the controls and specifically exclude functionality and data structures internal to the operation of the controls. Related control: SA-5.

(2) *ACQUISITION PROCESS | DESIGN / IMPLEMENTATION INFORMATION FOR SECURITY CONTROLS*

The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes: [*Selection (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; [Assignment: organization-defined design/implementation information*]] at [*Assignment: organization-defined level of detail*].

Deleted: /specifications

Deleted: and

Deleted: Developmental and evaluation

Deleted: assurance requirements.

Deleted: The acquisition documents for information systems, information system components, and information system services include, either explicitly or by reference, security requirements

Deleted: describe: (i) required

Deleted: (i.e.,

Deleted: needs

Deleted: , as necessary, specific

Deleted: controls and other specific FISMA

Deleted:); (ii) required design

Deleted: ; (iii) required test and evaluation

Deleted: ;

Deleted: (iv) required documentation. The requirements in the acquisition documents permit updating security controls as new threats/vulnerabilities are identified

Deleted: as new technologies are

Deleted: . Acquisition documents also include

Deleted: for appropriate information

Deleted: . The

Deleted: addresses

Deleted: system

Deleted: and information

Deleted: the

Deleted: in the information system.

Deleted: the

Deleted: categorization for the information system. In addition, the required documentation includes security

Deleted: and security implementation guidance. FISMA reporting instructions provide guidance on configuration requirements

Deleted: federal information systems.

Deleted: in acquisition documents that vendors/contractors provide information describing

Deleted: within the information system, information system components, or information system services in sufficient detail to permit analysis and testing of the controls

Deleted: in acquisition documents that vendors/contractors provide informati ...

Deleted: details of

Deleted: within the information syster ...

Supplemental Guidance: Organizations may require different levels of detail in design and implementation documentation for security controls employed in organizational information systems, system components, or information system services based on mission/business requirements, requirements for trustworthiness/resiliency, and requirements for analysis and testing. Information 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 multiple subsystems and the interfaces between subsystems providing security-relevant functionality. The low-level design for the system is expressed in terms of modules with particular emphasis on software and firmware (but not excluding hardware) and the interfaces between modules providing security-relevant functionality. Source code and hardware schematics are typically referred to as the implementation representation of the information system. Related control: SA-5.

Deleted: (including functional interfaces among control components) in sufficient detail to permit analysis and testing of the controls

(3) *ACQUISITION PROCESS | DEVELOPMENT METHODS / TECHNIQUES / PRACTICES*

The organization requires the developer of the information system, system component, or information system service to demonstrate the use of a system development life cycle that includes [*Assignment: organization-defined* state-of-the-practice *system/security engineering methods, software development methods, testing/evaluation/validation techniques, and quality control processes*].

Deleted: software vendors/manufacturers

Deleted: that their software

Deleted: processes employ

Deleted: software and

Supplemental Guidance: Following a well-defined system development life cycle that includes state-of-the-practice software development methods, systems/security engineering methods, quality control processes, and testing, evaluation, and validation techniques helps to reduce the number and severity of latent errors within information systems, system components, and information system services. Reducing the number/severity of such errors reduces the number of vulnerabilities in those systems, components, and services. Related control: SA-12.

Deleted: validation techniques to minimize flawed or malformed software

(4) *ACQUISITION PROCESS | ASSIGNMENT OF COMPONENTS TO SYSTEMS*

[Withdrawn: Incorporated into CM-8 (9)].

Deleted: The organization ensures that each information system component acquired is explicitly assigned to an information system, and that the owner of the system acknowledges this assignment.

(5) *ACQUISITION PROCESS | SYSTEM / COMPONENT / SERVICE CONFIGURATIONS*

The organization requires the developer of the information system, system component, or information system service to:

(a) Deliver the system, component, or service with [*Assignment: organization-defined security configurations*] implemented; and

(b) Use the configurations as the default for any subsequent system, component, or service reinstallation or upgrade.

Deleted: in acquisition documents, that

Deleted: components are delivered in a secure, documented configuration,

Deleted: that

Deleted: secure configuration is

Deleted: configuration

Deleted: software reinstalls

Deleted: upgrades

Supplemental Guidance: Security configurations include, for example, the U.S. Government Configuration Baseline (USGCB) and any limitations on functions, ports, protocols, and services. Security characteristics include, for example, requiring that all default passwords have been changed. Related control: CM-8.

(6) *ACQUISITION PROCESS | USE OF INFORMATION ASSURANCE PRODUCTS*

The organization:

(a) Employs only government off-the-shelf (GOTS) or commercial off-the-shelf (COTS) information assurance (IA) and IA-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

Deleted: composes

(b) Ensures that these products have been evaluated and/or validated by NSA or in accordance with NSA-approved procedures.

Deleted: the

Supplemental Guidance: COTS IA or IA-enabled information technology products used to protect classified information by cryptographic means may be required to use NSA-approved key management. Related controls: SC-8, SC-12, SC-13.

Deleted: Enhancement

Deleted: ,

(7) *ACQUISITION PROCESS | NIAP-APPROVED PROTECTION PROFILES*

The organization:

(a) Limits the use of commercially provided information assurance (IA) and IA-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

Deleted: validated U.S. Government

(b) Requires, 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.

Deleted: U.S. Government

Deleted: then

Supplemental Guidance: Related controls: SC-12, SC-13.

(8) *ACQUISITION PROCESS | CONTINUOUS MONITORING PLAN*

The organization requires the developer of the information system, system component, or information system service to produce a plan for the continuous monitoring of security control effectiveness that contains [*Assignment: organization-defined level of detail*].

Supplemental Guidance: The objective of continuous monitoring plans is to determine if the complete set of planned, required, and deployed security controls within the information system, system component, or information system service continue to be effective over time based on the inevitable changes that occur. Developer continuous monitoring plans include a sufficient level of detail such that the information can be incorporated into the continuous monitoring strategies and programs implemented by organizations. Related control: CA-7.

(9) *ACQUISITION PROCESS | FUNCTIONS / PORTS / PROTOCOLS / SERVICES IN USE*

The organization requires the developer of the information system, system component, or information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use.

Supplemental Guidance: The identification of functions, ports, protocols, and services early in the system development life cycle (e.g., during the initial requirements definition and design phases) allows organizations to influence the design of the information system, information system component, or information system service. This early involvement in the 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 information system service providers to do so). Early identification of functions, ports, protocols, and services avoids costly retrofitting of security controls after the information system, system component, or information system service has been implemented. SA-9 describes requirements for external information system services with organizations identifying which functions, ports, protocols, and services are provided from external sources. Related controls: CM-7, SA-9.

(10) *ACQUISITION PROCESS | USE OF APPROVED PIV PRODUCTS*

The organization employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.

Supplemental Guidance: Related controls: IA-2; IA-8.

References: HSPD-12; ISO/IEC 15408; FIPS Publications 140-2, 201; NIST Special Publications 800-23, 800-35, 800-36, 800-37, 800-64, 800-70, 800-137; Federal Acquisition Regulation; Web: www.niap-ccevs.org, fips201ep.cio.gov, www.acquisition.gov/far.

Priority and Baseline Allocation:

P1	**LOW** SA-4 (10)	**MOD** SA-4 (1) (2) (9) (10)	**HIGH** SA-4 (1) (2) (9) (10)

Deleted: 4

Deleted: 4

SA-5 INFORMATION SYSTEM DOCUMENTATION

Control: The organization:

a. Obtains administrator documentation for the information system, system component, or information system service that describes:

Deleted: , protects as required, and makes available to authorized personnel,

1. Secure configuration, installation, and operation of the system, component, or service;

Deleted: information

2. Effective use and maintenance of security functions/mechanisms; and

Deleted: features/

3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;

b. Obtains user documentation for the information system, system component, or information system service that describes:

1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;

2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and

3. User responsibilities in maintaining the security of the system, component, or service;

c. Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and [*Assignment: organization-defined actions*] in response;

d. Protects documentation as required, in accordance with the risk management strategy; and

e. Distributes documentation to [*Assignment: organization-defined personnel or roles*].

Supplemental Guidance: This control helps organizational personnel understand the implementation and operation of security controls associated with information systems, system components, and information system services. Organizations consider establishing specific measures to determine the quality/completeness of the content provided. The inability to obtain needed documentation may occur, for example, due to the age of the information system/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 effective implementation or operation of security controls. The level of protection provided for selected information system, component, or service documentation is commensurate with the security category or classification of the system. For example, documentation associated with a key DoD weapons system or command and control system would typically require a higher level of protection than a routine administrative system. Documentation that addresses information system vulnerabilities may also require an increased level of protection. Secure operation of the information system, includes, for example, initially starting the system and resuming secure system operation after any lapse in system operation. Related controls: CM-6, CM-8, PL-2, PL-4, PS-2, SA-3, SA-4.

Control Enhancements:

(1) *INFORMATION SYSTEM DOCUMENTATION | FUNCTIONAL PROPERTIES OF SECURITY CONTROLS*
[Withdrawn: Incorporated into SA-4 (1)].

(2) *INFORMATION SYSTEM DOCUMENTATION | SECURITY-RELEVANT EXTERNAL SYSTEM INTERFACES*
[Withdrawn: Incorporated into SA-4 (2)].

(3) *INFORMATION SYSTEM DOCUMENTATION | HIGH-LEVEL DESIGN*
[Withdrawn: Incorporated into SA-4 (2)].

(4) *INFORMATION SYSTEM DOCUMENTATION | LOW-LEVEL DESIGN*

(5) [Withdrawn: Incorporated into SA-4 (2)]. *INFORMATION SYSTEM DOCUMENTATION | SOURCE CODE*
[Withdrawn: Incorporated into SA-4 (2)].

References: None.

Priority and Baseline Allocation:

P2	**LOW** SA-5	**MOD** SA-5	**HIGH** SA-5

SA-6 SOFTWARE USAGE RESTRICTIONS

[Withdrawn: Incorporated into CM-10 and SI-7].

d.

Deleted: and

Deleted: , protects as required, and makes available to authorized personnel,

Deleted: features/

Deleted: features/

Deleted: with the information system

Deleted: information and information

Deleted: ; and

Deleted: .

Deleted: of the organization

Deleted: necessary information system

Deleted: and/

Deleted: the vendor/contractor.

Deleted: information system

Deleted: and/or operation of security controls

Deleted: The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing.¶

Deleted: <#>The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the high-level design of the information system in terms of subsystems and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing.¶

Deleted: The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the high-level design of the information system in terms of subsystems and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing.¶
Enhancement Supplemental Guidance: An information system can be partitioned into multiple subsystems.¶

Deleted: The organization obtains, protects as required, and makes ...

Deleted: <#>The organization obtains, protects as required, and makes ...

Deleted: (1) (3)

Deleted: (1) (2) (3)

Deleted: Control: The organization:¶ ...

Moved up [6]: software and associated documentation protected by quantity licenses ...

e.

SA-7 USER-INSTALLED SOFTWARE

[Withdrawn: Incorporated into CM-11 and SI-7].

SA-8 SECURITY ENGINEERING PRINCIPLES

Control: The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.

Supplemental Guidance: Organizations apply security engineering principles primarily to new development information systems or systems undergoing major upgrades. For legacy systems, organizations apply security engineering principles to system upgrades and modifications to the extent feasible, given the current state of hardware, software, and firmware within those systems. Security engineering principles include, for example: (i) developing layered protections; (ii) establishing sound security policy, architecture, and controls as the foundation for design; (iii) incorporating security requirements into the system development life cycle; (iv) delineating physical and logical security boundaries; (v) ensuring that system developers are trained on how to build secure software; (vi) tailoring security controls to meet organizational and operational needs; (vii) performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk; and (viii) reducing risk to acceptable levels, thus enabling informed risk management decisions. Related controls: PM-7, SA-3, SA-4, SA-17, SC-2, SC-3.

Control Enhancements: None.

References: NIST Special Publication 800-27.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SA-8	**HIGH** SA-8

SA-9 EXTERNAL INFORMATION SYSTEM SERVICES

Control: The organization:

a. Requires that providers of external information system services comply with organizational information security requirements and employ [*Assignment: organization-defined security controls*] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;

b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and

c. Employs [*Assignment: organization-defined processes, methods, and techniques*] to monitor security control compliance by external service providers on an ongoing basis.

Supplemental Guidance: External information system services are services that are implemented outside of the authorization boundaries of organizational information systems. This includes services that are used by, but not a part of, organizational information systems. FISMA and OMB policy require that organizations using external service providers that are processing, storing, or

Deleted: Supplemental Guidance: Tracking systems can include, for example, simple spreadsheets or fully automated, specialized applications depending on the needs of the organization.¶

Moved up [9]: References: None.¶
Priority and Baseline Allocation:¶

Deleted: The organization:¶
<#>Prohibits the use of binary or machine executable code from sources with limited or no warranty without accompanying source code; and¶
<#>Provides exceptions to the source code requirement only for compelling mission/operational requirements when no alternative solutions are available and with the express written consent of the authorizing official.¶
Enhancement Supplemental Guidance: Software products without accompanying source code from sources with limited or no warranty are assessed for potential security impacts. The assessment addresses the fact that these types of software products are difficult or impossible to review, repair, or extend, given that the organization does not have access to the origi ...

Deleted: P1 ...

Deleted: Control: The organization enforces ...

Moved up [7]: References: None.¶ ...

Deleted: P1 ...

Deleted: The application of

Deleted: is

Deleted: targeted at

Deleted: and is integrated into the system ...

Deleted: information

Deleted: the organization applies

Deleted: the

Deleted: the system. Examples of security

Deleted: and integrators

Deleted: develop

Deleted: and (vii

Deleted: appropriate

Deleted: Monitors

Deleted: An external

Deleted: service is a service

Deleted: is

Deleted: boundary

Deleted: the

Deleted: system (i.e., a service

Deleted: is

Deleted: the

Deleted: system). Relationships

transmitting federal information or operating information systems on behalf of the federal government ensure that such providers meet the same security requirements that federal agencies are required to meet. Organizations establish relationships with external service providers in a variety of ways including, for example, through joint ventures, business partnerships, contracts, interagency agreements, lines of business arrangements, licensing agreements, and supply chain exchanges. The responsibility for managing risks from the use of external information system services remains with authorizing officials. For services external to organizations, a chain of trust requires that organizations establish and retain a level of confidence that each participating provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered. The extent and nature of this chain of trust varies based on the relationships between organizations and the external providers. Organizations document the basis for trust relationships so the relationships can be monitored over time. External information 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 security controls, describe measurable outcomes, and identify remedies and response requirements for identified instances of noncompliance. Related controls: CA-3, IR-7, PS-7.

Control Enhancements:

(1) *EXTERNAL INFORMATION SYSTEMS | RISK ASSESSMENTS / ORGANIZATIONAL APPROVALS*

The organization:

(a) Conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services; and

(b) Ensures that the acquisition or outsourcing of dedicated information security services is approved by [*Assignment: organization-defined personnel or roles*].

Supplemental Guidance: Dedicated information security services include, for example, incident monitoring, analysis and response, operation of information security-related devices such as firewalls, or key management services. Related controls: CA-6, RA-3.

(2) *EXTERNAL INFORMATION SYSTEMS | IDENTIFICATION OF FUNCTIONS / PORTS / PROTOCOLS / SERVICES*

The organization requires providers of [*Assignment: organization-defined external information system services*] to identify the functions, ports, protocols, and other services required for the use of such services.

Supplemental Guidance: Information from external service providers regarding the specific functions, ports, protocols, and services used in the provision of such services can be particularly useful when the need arises to understand the trade-offs involved in restricting certain functions/services or blocking certain ports/protocols. Related control: CM-7.

(3) *EXTERNAL INFORMATION SYSTEMS | ESTABLISH / MAINTAIN TRUST RELATIONSHIP WITH PROVIDERS*

The organization establishes, documents, and maintains trust relationships with external service providers based on [*Assignment: organization-defined security requirements, properties, factors, or conditions defining acceptable trust relationships*].

Supplemental Guidance: The degree of confidence that the risk from using external services is at an acceptable level depends on the trust that organizations place in the external providers, individually or in combination. Trust relationships can help organization to gain increased levels of confidence that participating service providers are providing adequate protection for the services rendered. Such relationships can be complicated due to the number of potential entities participating in the consumer-provider interactions, subordinate relationships and levels of trust, and the types of interactions between the parties. In some cases, the degree of trust is based on the amount of direct control organizations are able to exert on external service providers with regard to employment of security controls necessary for the protection of the service/information and the evidence brought forth as to the effectiveness of those controls. The level of control is typically established by the terms and conditions of the contracts or service-level agreements and can range from extensive control (e.g., negotiating contracts or agreements that specify security requirements for the providers) to very limited control (e.g., using contracts or service-level agreements to obtain commodity services such as commercial telecommunications services). In other cases, levels of trust are based on factors

Deleted: are established

Deleted: outsourcing arrangements (i.e.,

Deleted:),

Deleted: /or

Deleted:

Deleted: adequately mitigating

Deleted: arising

Deleted: the

Deleted: official. Authorizing

Deleted: require that an appropriate chain of trust be established with external service providers when dealing with the many issues associated with information security.

Deleted: the organization

Deleted: the organization

Deleted: to the organization.

Deleted: relationship

Deleted: the organization and the external provider. Where a sufficient level of trust cannot be established in the external services and/or service providers, the organization employs compensating security controls or accepts the greater degree of risk. The external

Deleted: provider, and

Deleted: any

Deleted:

Deleted: the

Deleted: each required

Deleted: control

Deleted: any

Deleted: instance

Deleted: ***senior organizational official***

Deleted: Enhancement

that convince organizations that required security controls have been employed and that determinations of control effectiveness exist. For example, separately authorized external information system services provided to organizations through well-established business relationships may provide degrees of trust in such services within the tolerable risk range of the organizations using the services. External service providers may also outsource selected services to other external entities, making the trust relationship more difficult and complicated to manage. Depending on the nature of the services, organizations may find it very difficult to place significant trust in external providers. This is not due to any inherent untrustworthiness on the part of providers, but to the intrinsic level of risk in the services.

(4) *EXTERNAL INFORMATION SYSTEMS | CONSISTENT INTERESTS OF CONSUMERS AND PROVIDERS*

The organization employs [*Assignment: organization-defined security safeguards*] to ensure that the interests of [*Assignment: organization-defined external service providers*] are consistent with and reflect organizational interests.

Supplemental Guidance: As organizations increasingly use external service providers, the possibility exists that the interests of the service providers may diverge from organizational interests. In such situations, simply having the correct technical, procedural, or operational safeguards in place may not be sufficient if the service providers that implement and control those safeguards are not operating in a manner consistent with the interests of the consuming organizations. Possible 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 (i.e., providers with which organizations have had positive experiences), and conducting periodic/unscheduled visits to service provider facilities.

(5) *EXTERNAL INFORMATION SYSTEMS | PROCESSING, STORAGE, AND SERVICE LOCATION*

The organization restricts the location of [*Selection (one or more): information processing; information/data; information system services*] to [*Assignment: organization-defined locations*] based on [*Assignment: organization-defined requirements or conditions*].

Supplemental Guidance: The location of information processing, information/data storage, or information system services that are critical to organizations can have a direct impact on the ability of those organizations to successfully execute their missions/business functions. This situation exists when external providers control the location of processing, storage or services. The criteria external providers use for the selection of processing, storage, or service locations may be different from organizational criteria. For example, organizations may want to ensure that data/information storage locations are restricted to certain locations to facilitate incident response activities (e.g., forensic analyses, after-the-fact investigations) in case of information security breaches/compromises. Such incident response activities may be adversely affected by the governing laws or protocols in the locations where processing and storage occur and/or the locations from which information system services emanate.

References: NIST Special Publication 800-35.

Priority and Baseline Allocation:

P1	**LOW** SA-9	**MOD** SA-9 (2)	**HIGH** SA-9 (2)

SA-10 DEVELOPER CONFIGURATION MANAGEMENT

Control: The organization requires the developer of the information system, system component, or information system service to:

a. Perform configuration management during system, component, or service [*Selection (one or more): design; development; implementation; operation*];

b. Document, manage, and control the integrity of changes to [*Assignment: organization-defined configuration items under configuration management*];

Deleted: _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

Deleted: that

Deleted: developers/integrators

Deleted: information system

Deleted: ,

Deleted: ,

Deleted: , and

Deleted: ;

Deleted: Manage

Deleted: the information system;

c. Implement only organization-approved changes to the system, component, or service;

d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and

Deleted: information system

e. Track security flaws and flaw resolution within the system, component, or service and report findings to [*Assignment: organization-defined personnel*].

Deleted: .

Supplemental Guidance: This control also applies to organizations conducting internal information systems development and integration. Organizations consider the quality and completeness of the configuration management activities conducted by developers as evidence of applying effective security safeguards. Safeguards include, for example, protecting from unauthorized modification or destruction, the master copies of all material used to generate security-relevant portions of the system hardware, software, and firmware. Maintaining the integrity of changes to the information system, information system component, or information system service requires configuration control throughout the system development life cycle to track authorized changes and prevent unauthorized changes. Configuration items that are placed under configuration management (if existence/use is required by other security controls) include: the formal model; the functional, high-level, and low-level design specifications; other design data; implementation documentation; source code and hardware schematics; the running version of the object code; tools for comparing new versions of security-relevant hardware descriptions and software/firmware source code with previous versions; and test fixtures and documentation. Depending on the mission/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 life cycle. Related controls: CM-3, CM-4, CM-9, SA-12, SI-2.

Control Enhancements:

(1) *DEVELOPER CONFIGURATION MANAGEMENT | SOFTWARE / FIRMWARE INTEGRITY VERIFICATION*

The organization requires the developer of the information system, system component, or information system service to enable integrity verification of software and firmware components.

Supplemental Guidance: This control enhancement allows organizations to detect unauthorized changes to software and firmware components through the use of tools, techniques, and/or mechanisms provided by developers. Integrity checking mechanisms can also address counterfeiting of software and firmware components. Organizations verify the integrity of software and firmware components, for example, through secure one-way hashes provided by developers. Delivered software and firmware components also include any updates to such components. Related control: SI-7.

Deleted: that

Deleted: developers/integrators provide an integrity check of software

Deleted: facilitate organizational

Deleted: integrity after delivery

Deleted: The organization provides an

(2) *DEVELOPER CONFIGURATION MANAGEMENT | ALTERNATIVE CONFIGURATION MANAGEMENT PROCESSES*

The organization provides an alternate configuration management process using organizational personnel in the absence of a dedicated developer configuration management team.

Supplemental Guidance: Alternate configuration management processes may be required, for example, when organizations use commercial off-the-shelf (COTS) information technology products. Alternate configuration management processes include organizational personnel that: (i) are responsible for reviewing/approving proposed changes to information systems, system components, and information system services; and (ii) conduct security impact analyses prior to the implementation of any changes to systems, components, or services (e.g., a configuration control board that considers security impacts of changes during development and includes representatives of both the organization and the developer, when applicable).

Deleted: with

Deleted: /integrator

Deleted: Enhancement

Deleted: The

Deleted: process includes key

Deleted: and

Deleted: the

Deleted: security personnel that

Deleted: the system.

(3) *DEVELOPER CONFIGURATION MANAGEMENT | HARDWARE INTEGRITY VERIFICATION*

The organization requires the developer of the information system, system component, or information system service to enable integrity verification of hardware components.

Supplemental Guidance: This control enhancement allows organizations to detect unauthorized changes to hardware components through the use of tools, techniques, and/or mechanisms provided by developers. Organizations verify the integrity of hardware components, for example, with hard-to-copy labels and verifiable serial numbers provided by developers, and by requiring the implementation of anti-tamper technologies. Delivered hardware components also include updates to such components. Related control: SI-7.

(4) *DEVELOPER CONFIGURATION MANAGEMENT | TRUSTED GENERATION*

The organization requires the developer of the information system, system component, or information system service to employ tools for comparing newly generated versions of security-relevant hardware descriptions and software/firmware source and object code with previous versions.

Supplemental Guidance: This control enhancement addresses changes to hardware, software, and firmware components between versions during development. In contrast, SA-10 (1) and SA-10 (3) allow organizations to detect unauthorized changes to hardware, software, and firmware components through the use of tools, techniques, and/or mechanisms provided by developers.

(5) *DEVELOPER CONFIGURATION MANAGEMENT | MAPPING INTEGRITY FOR VERSION CONTROL*

The organization requires the developer of the information system, system component, or information system service to maintain the integrity of the mapping between the master build data (hardware drawings and software/firmware code) describing the current version of security-relevant hardware, software, and firmware and the on-site master copy of the data for the current version.

Supplemental Guidance: This control enhancement addresses changes to hardware, software, and firmware components during initial development and during system life cycle updates. Maintaining the integrity between the master copies of security-relevant hardware, software, and firmware (including designs and source code) and the equivalent data in master copies on-site in operational environments is essential to ensure the availability of organizational information systems supporting critical missions and/or business functions.

(6) *DEVELOPER CONFIGURATION MANAGEMENT | TRUSTED DISTRIBUTION*

The organization requires the developer of the information system, system component, or information system service to execute procedures for ensuring that security-relevant hardware, software, and firmware updates distributed to the organization are exactly as specified by the master copies.

Supplemental Guidance: The trusted distribution of security-relevant hardware, software, and firmware updates helps to ensure that such updates are faithful representations of the master copies maintained by the developer and have not been tampered with during distribution.

References: NIST Special Publication 800-128.

Deleted: None

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SA-10	**HIGH** SA-10

SA-11 DEVELOPER SECURITY TESTING AND EVALUATION

Control: The organization requires the developer of the information system, system component, or information system service to:

Deleted: that

Deleted: developers/integrators, in consultation with associated security personnel (including security engineers):

a. Create and implement a security assessment plan;

Deleted: test and

b. Perform [*Selection (one or more): unit; integration; system; regression*] testing/evaluation at [*Assignment: organization-defined depth and coverage*];

Deleted: plan;

c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;

d. Implement a verifiable flaw remediation process; and

Deleted: to correct weaknesses

e. Correct flaws identified during security testing/evaluation.

Deleted: deficiencies

Deleted: the

Deleted: and

Supplemental Guidance: Developmental security testing/evaluation occurs at all post-design phases of the system development life cycle. Such testing/evaluation confirms that the required security controls are implemented correctly, operating as intended, enforcing the desired security policy, and meeting established security requirements. Security properties of information systems may be affected by the interconnection of system components or changes to those components. These interconnections or changes (e.g., upgrading or replacing applications and operating systems) may adversely affect previously implemented security controls. This control provides additional types of security testing/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 employ these analysis approaches in a variety of tools (e.g., web-based application scanners, static analysis tools, binary analyzers) and in source code reviews. Security assessment plans provide the specific activities that developers plan to carry out including the types of analyses, testing, evaluation, and reviews of software and firmware components, the degree of rigor to be applied, and the types of artifacts produced during those processes. The *depth* of security testing/evaluation refers to the rigor and level of detail associated with the assessment process (e.g., black box, gray box, or white box testing). The *coverage* of security testing/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 assessment plans, flaw remediation processes, and the evidence that the plans/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 information system. Contracts may specify documentation requirements. Related controls: CA-2, CM-4, SA-3, SA-4, SA-5, SI-2.

Deleted: ; and

Control Enhancements:

Deleted: <#>Document the results of the security testing/evaluation and flaw remediation processes.¶

Supplemental Guidance: Developmental security test results are used to the greatest extent feasible after verification of the results and recognizing that these results are impacted whenever there have been security-relevant modifications to the information system subsequent to developer testing. Test results may be used in support of the security authorization process for the delivered information system. Related control: CA-2, SI-2.¶

(1) *DEVELOPER SECURITY TESTING AND EVALUATION | STATIC CODE ANALYSIS*

The organization requires the developer of the information system, system component, or information system service to employ static code analysis tools to identify common flaws and document the results of the analysis.

Deleted: that

Deleted: developers/integrators

Deleted: examine software for

Supplemental Guidance: Static code analysis provides a technology and methodology for security reviews. Such analysis can be used to identify security vulnerabilities and enforce security 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 fixed. An excessively high density of ignored findings (commonly referred to as ignored or false positives) indicates a potential problem with the analysis process or tool. In such cases, organizations weigh the validity of the evidence against evidence from other sources.

Deleted: The organization requires that information system developers/integrators create a security test

(2) *DEVELOPER SECURITY TESTING AND EVALUATION | THREAT AND VULNERABILITY ANALYSES*

The organization requires the developer of the information system, system component, or information system service to perform threat and vulnerability analyses and subsequent testing/evaluation of the as-built system, component, or service.

Deleted: <#>The organization requires that information system developers/integrators perform a vulnerability analysis to document vulnerabilities, exploitation potential, and risk mitigations.¶

Supplemental Guidance: Applications may deviate significantly from the functional and design specifications created during the requirements and design phases of the system development life cycle. Therefore, threat and vulnerability analyses of information systems, system components, and information system services prior to delivery are critical to the effective operation of those systems, components, and services. Threat and vulnerability analyses at this phase of the life cycle help to ensure that design or implementation changes have been accounted for, and that any new vulnerabilities created as a result of those changes have been reviewed and mitigated. Related controls: PM-15, RA-5.

(3) *DEVELOPER SECURITY TESTING AND EVALUATION | INDEPENDENT VERIFICATION OF ASSESSMENT PLANS / EVIDENCE*

The organization:

(a) Requires an independent agent satisfying [*Assignment: organization-defined independence criteria*] to verify the correct implementation of the developer security assessment plan and the evidence produced during security testing/evaluation; and

Deleted: verification and validation

Deleted: .

(b) Ensures that the independent agent either is provided with sufficient information to complete the verification process or has been granted the authority to obtain such information.

Supplemental Guidance: Independent agents have the necessary qualifications (i.e., expertise, skills, training, and experience) to verify the correct implementation of developer security assessment plans. Related controls: AT-3, CA-7, RA-5, SA-12.

(4) *DEVELOPER SECURITY TESTING AND EVALUATION | MANUAL CODE REVIEWS*

The organization requires the developer of the information system, system component, or information system service to perform a manual code review of [Assignment*: organization-defined specific code*] using [*Assignment: organization-defined processes, procedures, and/or techniques*].

Supplemental Guidance: Manual code reviews are usually reserved for the critical software and firmware components of information systems. Such code reviews are uniquely effective at identifying weaknesses that require knowledge of the application's requirements or context which are generally unavailable to more automated analytic tools and techniques such as static or 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.

(5) *DEVELOPER SECURITY TESTING AND EVALUATION | PENETRATION TESTING / ANALYSIS*

The organization requires the developer of the information system, system component, or information system service to perform penetration testing at [*Assignment: organization-defined breadth/depth*] and with [*Assignment: organization-defined constraints*].

Supplemental Guidance: Penetration testing is an assessment methodology in which assessors, using all available information technology product and/or information system documentation (e.g., product/system design specifications, source code, and administrator/operator manuals) and working under specific constraints, attempt to circumvent implemented security features of information technology products and information systems. Penetration testing can include, for example, white, gray, or black box testing with analyses performed by skilled security professionals simulating adversary actions. The objective of penetration testing is to uncover potential vulnerabilities in information technology products and information systems resulting from implementation errors, configuration faults, or other operational deployment weaknesses or deficiencies. Penetration tests can be performed in conjunction with automated and manual code reviews to provide greater levels of analysis than would ordinarily be possible.

(6) *DEVELOPER SECURITY TESTING AND EVALUATION | ATTACK SURFACE REVIEWS*

The organization requires the developer of the information system, system component, or information system service to perform attack surface reviews.

Supplemental Guidance: Attack surfaces of information systems are exposed areas that make those systems more vulnerable to cyber attacks. This includes any accessible areas where weaknesses or deficiencies in information systems (including the hardware, software, and firmware components) provide opportunities for adversaries to exploit vulnerabilities. Attack surface reviews ensure that developers: (i) analyze both design and implementation changes to information systems; and (ii) mitigate attack vectors generated as a result of the changes. Correction of identified flaws includes, for example, deprecation of unsafe functions.

(7) *DEVELOPER SECURITY TESTING AND EVALUATION | VERIFY SCOPE OF TESTING / EVALUATION*

The organization requires the developer of the information system, system component, or information system service to verify that the scope of security testing/evaluation provides complete coverage of required security controls at [*Assignment: organization-defined depth of testing/evaluation*].

Supplemental Guidance: Verifying that security testing/evaluation provides complete coverage of required security controls can be accomplished by a variety of analytic techniques ranging from informal to formal. Each of these techniques provides an increasing level of assurance corresponding to the degree of formality of the analysis. Rigorously demonstrating security control coverage at the highest levels of assurance can be provided by the use of formal modeling and analysis techniques including correlation between control implementation and corresponding test cases.

(8) *DEVELOPER SECURITY TESTING AND EVALUATION | DYNAMIC CODE ANALYSIS*

The organization requires the developer of the information system, system component, or information system service to employ dynamic code analysis tools to identify common flaws and document the results of the analysis.

Supplemental Guidance: Dynamic code analysis provides run-time verification of software programs, using tools capable of monitoring programs for memory corruption, user privilege issues, and other potential security problems. Dynamic code analysis employs run-time tools to help to ensure that security functionality performs in the manner in which 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 functional and design specifications for the applications.

References: ISO/IEC 15408; NIST Special Publication 800-53A; Web: nvd.nist.gov, cwe.mitre.org, cve.mitre.org, capec.mitre.org.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SA-11	**HIGH** SA-11

Deleted: P2

SA-12 SUPPLY CHAIN PROTECTION

Control: The organization protects against supply chain threats to the information system, system component, or information system service by employing [*Assignment: organization-defined security safeguards*] as part of a comprehensive, defense-in-breadth information security strategy.

Deleted: :

Deleted: *list of measures to protect against supply chain threats*

Supplemental Guidance: Information systems (including system components that compose those systems) need to be protected throughout the system development life cycle (i.e., during design, development, manufacturing, packaging, assembly, distribution, system integration, operations, maintenance, and retirement). Protection of organizational information systems is accomplished through threat awareness, by the identification, management, and reduction of vulnerabilities at each phase of the life cycle and the use of complementary, mutually reinforcing strategies to respond to risk. Organizations consider implementing a standardized process to address supply chain risk with respect to information systems and system components, and to educate the acquisition workforce on threats, risk, and required security controls. Organizations use the acquisition/procurement processes to require supply chain entities to implement necessary security safeguards to: (i) reduce the likelihood of unauthorized modifications at each stage in the supply chain; and (ii) protect information systems and information system components, prior to taking delivery of such systems/components. This control enhancement also applies to information system services. Security safeguards include, for example: (i) security controls for development systems, development facilities, and external connections to development systems; (ii) vetting development personnel; and (iii) use of tamper-evident packaging during shipping/warehousing. 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. Related controls: AT-3, CM-8, IR-4, PE-16, PL-8, SA-3, SA-4, SA-8, SA-10, SA-14, SA-15, SA-18, SA-19, SC-29, SC-30, SC-38, SI-7.

Deleted: A defense-in-breadth approach helps to protect information

Deleted: the information technology products

Deleted: and

Deleted: This

Deleted: elimination

Deleted: mitigate risk

Control Enhancements:

(1) *SUPPLY CHAIN PROTECTION | ACQUISITION STRATEGIES / TOOLS / METHODS*

The organization employs [*Assignment: organization-defined tailored acquisition strategies, contract tools, and procurement methods*] for the purchase of the information system, system component, or information system service from suppliers.

Deleted: purchases

Supplemental Guidance: The use of acquisition and procurement processes by organizations early in the system development life cycle provides an important vehicle to protect the supply chain. Organizations use available all-source intelligence analysis to inform the tailoring of acquisition strategies, tools, and methods. There are a number of different tools and techniques available (e.g., obscuring the end use of an information system or system

Deleted: anticipated

component, using blind or filtered buys). Organizations also consider creating incentives for suppliers who: (i) implement required security safeguards; (ii) promote transparency into their organizational processes and security practices; (iii) provide additional vetting of the processes and security practices of subordinate suppliers, critical information system components, and services; (iv) restrict purchases from specific suppliers or countries; and (v) provide contract language regarding the prohibition of tainted or counterfeit components. In addition, organizations consider minimizing the time between purchase decisions and required delivery to limit opportunities for adversaries to corrupt information system components or products. Finally, organizations can use trusted/controlled distribution, delivery, and warehousing options to reduce supply chain risk (e.g., requiring tamper-evident packaging of information system components during shipping and warehousing). Related control: SA-19.

(2) *SUPPLY CHAIN PROTECTION | SUPPLIER REVIEWS*

The organization conducts a supplier review prior to entering into a contractual agreement to acquire the information system, system component, or information system service.

Supplemental Guidance: Supplier reviews include, for example: (i) analysis of supplier processes used to design, develop, test, implement, verify, deliver, and support information systems, system components, and information system services; and (ii) assessment of supplier training and experience in developing systems, components, or services with the required security capability. These reviews provide organizations with increased levels of visibility into supplier activities during the system development life cycle to promote more effective supply chain risk management. Supplier reviews can also help to determine whether primary suppliers have security safeguards in place and a practice for vetting subordinate suppliers, for example, second- and third-tier suppliers, and any subcontractors.

(3) *SUPPLY CHAIN PROTECTION | TRUSTED SHIPPING AND WAREHOUSING*

[Withdrawn: Incorporated into SA-12 (1)].

(4) *SUPPLY CHAIN PROTECTION | DIVERSITY OF SUPPLIERS*

[Withdrawn: Incorporated into SA-12 (13)].

(5) *SUPPLY CHAIN PROTECTION | LIMITATION OF HARM*

(6) **The organization employs [*Assignment:* organization-defined security safeguards] to limit harm from potential adversaries identifying and targeting the organizational supply chain.**

Supplemental Guidance: Supply chain risk is part of the advanced persistent threat (APT). Security safeguards and countermeasures to reduce the probability of adversaries successfully identifying and targeting the supply chain include, for example: (i) avoiding the purchase of custom configurations to reduce the risk of acquiring information systems, components, or products that have been corrupted via supply chain actions targeted at specific organizations; (ii) employing a diverse set of suppliers to limit the potential harm from any given supplier in the supply chain; (iii) employing approved vendor lists with standing reputations in industry, and (iv) using procurement carve outs (i.e., exclusions to commitments or obligations).

(7) *SUPPLY CHAIN PROTECTION | MINIMIZING PROCUREMENT TIME*

[Withdrawn: Incorporated into SA-12 (1)].

(8) *SUPPLY CHAIN PROTECTION | ASSESSMENTS PRIOR TO SELECTION / ACCEPTANCE / UPDATE*

The organization conducts an assessment of the information system, system component, or information system service prior to selection, acceptance, or update.

Supplemental Guidance: Assessments include, for example, testing, evaluations, reviews, and analyses. Independent, third-party entities or organizational personnel conduct assessments of systems, components, products, tools, and services. Organizations conduct assessments to uncover unintentional vulnerabilities and intentional vulnerabilities including, for example, malicious code, malicious processes, defective software, and counterfeits. Assessments can include, for example, static analyses, dynamic analyses, simulations, white, gray, and black box testing, fuzz testing, penetration testing, and ensuring that components or services are genuine (e.g., using tags, cryptographic hash verifications, or digital signatures). Evidence generated during security assessments is documented for follow-on actions carried out by organizations. Related controls: CA-2, SA-11.

(9) *SUPPLY CHAIN PROTECTION | USE OF ALL-SOURCE INTELLIGENCE*

Deleted: and spares in the initial acquisition.

Deleted: Enhancement Supplemental Guidance: Stockpiling information system components and spares avoids the need to use less trustworthy secondary or resale markets in future years.¶

Deleted: due diligence

Deleted: of suppliers

Deleted: agreements

Deleted: hardware, software, firmware

Deleted: services

Deleted: Enhancement Supplemental Guidance: The organization reviews supplier claims with regard to the use of appropriate security processes in the development and manufacture of information system components or products.¶

Deleted: The organization uses

Deleted: trusted shipping and warehousing for information systems, information system components, and information technology products.

Deleted: Enhancement Supplemental Guidance: Trusted shipping and warehousing reduces opportunities for subversive activities or interception during transit. Examples of supporting techniques include the use of a geographically aware beacon to detect shipment diversions or delays. Related control: PE-16.¶

Deleted: The organization employs a diverse set of suppliers for information systems, information system components, information technology products, and information system services. ¶
Enhancement Supplemental Guidance: Diversification of suppliers is intended to limit the potential harm from a given supplier in a supply chain, increasing the work factor for an adversary.

Deleted: employs standard configurations for information systems, information system components, and information technology products

Deleted: for information systems, information system components, and information technology products, the organization limits

Deleted: possibility

Deleted: and

Deleted: the

Deleted: organization.

Deleted: <#>The organization minimizes the time between purchase decisions and delivery of information systems, ...

Deleted: employs independent analysis and penetration testing against delivered

The organization uses all-source intelligence analysis of suppliers and potential suppliers of the information system, system component, or information system service.

Supplemental Guidance: All-source intelligence analysis is employed by organizations to inform engineering, acquisition, and risk management decisions. All-source intelligence consists of intelligence products and/or organizations and activities that incorporate all sources of information, most frequently including human intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence, and open source data in the production of finished intelligence. Where available, such information is used to analyze the risk of both intentional and unintentional vulnerabilities from development, manufacturing, and delivery processes, people, and the environment. This review is performed on suppliers at multiple tiers in the supply chain sufficient to manage risks. Related control: SA-15.

(10) *SUPPLY CHAIN PROTECTION | OPERATIONS SECURITY*

The organization employs [*Assignment: organization-defined Operations Security (OPSEC) safeguards*] in accordance with classification guides to protect supply chain-related information for the information system, system component, or information system service.

Supplemental Guidance: Supply chain information includes, for example: user identities; uses for information systems, information system components, and information system services; supplier identities; supplier processes; security requirements; design specifications; testing and evaluation results; and system/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: (i) identify those actions that can be observed by potential adversaries; (ii) determine indicators that adversaries might obtain that could be interpreted or pieced together to derive critical information in sufficient time to cause harm to organizations; (iii) implement safeguards or countermeasures to eliminate or reduce to an acceptable level, exploitable vulnerabilities; and (iv) consider how aggregated information may compromise the confidentiality of users or uses of the supply chain. OPSEC may require organizations to withhold critical mission/business information from suppliers and may include the use of intermediaries to hide the end use, or users, of information systems, system components, or information system services. Related control: PE-21.

(11) *SUPPLY CHAIN PROTECTION | VALIDATE AS GENUINE AND NOT ALTERED*

The organization employs [*Assignment: organization-defined security safeguards*] to validate that the information system or system component received is genuine and has not been altered.

Supplemental Guidance: For some information system components, especially hardware, there are technical means to help determine if the components are genuine or have been altered. Security safeguards used to validate the authenticity of information systems and information system components include, for example, optical/nanotechnology tagging and side-channel analysis. For hardware, detailed bill of material information can highlight the elements with embedded logic complete with component and production location.

(12) *SUPPLY CHAIN PROTECTION | PENETRATION TESTING / ANALYSIS OF ELEMENTS, PROCESSES, AND ACTORS*

The organization employs [*Selection (one or more): organizational analysis, independent third-party analysis, organizational penetration testing, independent third-party penetration testing*] of [*Assignment: organization-defined supply chain elements, processes, and actors*] associated with the *information system, system component, or information system service.*

Supplemental Guidance: This control enhancement addresses analysis and/or testing of the supply chain, not just delivered items. Supply chain elements are information technology products or product components that contain programmable logic and that are critically important to information system functions. Supply chain processes include, for example: (i) hardware, software, and firmware development processes; (ii) shipping/handling procedures; (iii) personnel and physical security programs; (iv) configuration management tools/measures to maintain provenance; or (v) any other programs, processes, or procedures associated with the production/distribution of supply chain elements. Supply chain actors are individuals with specific roles and responsibilities in the supply chain. The evidence generated during analyses and testing of supply chain elements, processes, and actors is documented and used to inform organizational risk management activities and decisions. Related control: RA-5.

(13) *SUPPLY CHAIN PROTECTION | INTER-ORGANIZATIONAL AGREEMENTS*

The organization establishes inter-organizational agreements and procedures with entities involved in the supply chain for the information system, system component, or information system service.

Supplemental Guidance: The establishment of inter-organizational agreements and procedures provides for notification of supply chain compromises. Early notification of supply chain compromises that can potentially adversely affect or have adversely affected organizational information systems, including critical system components, is essential for organizations to provide appropriate responses to such incidents.

(14) *SUPPLY CHAIN PROTECTION | CRITICAL INFORMATION SYSTEM COMPONENTS*

The organization employs [*Assignment: organization-defined security safeguards*] to ensure an adequate supply of [*Assignment: organization-defined critical information system components*].

Supplemental Guidance: Adversaries can attempt to impede organizational operations by disrupting the supply of critical information system components or corrupting supplier operations. Safeguards to ensure adequate supplies of critical information system components include, for example: (i) the use of multiple suppliers throughout the supply chain for the identified critical components; and (ii) stockpiling of spare components to ensure operation during mission-critical times.

(15) *SUPPLY CHAIN PROTECTION | IDENTITY AND TRACEABILITY*

The organization establishes and retains unique identification of [*Assignment: organization-defined supply chain elements, processes, and actors*] for the information system, system component, or information system service.

Supplemental Guidance: Knowing who and what is in the supply chains of organizations is critical to gaining visibility into what is happening within such supply chains, as well as monitoring and identifying high-risk events and activities. Without reasonable visibility and traceability into supply chains (i.e., elements, processes, and actors), it is very difficult for organizations to understand and therefore manage risk, and to reduce the likelihood of adverse events. Uniquely identifying acquirer and integrator roles, organizations, personnel, mission and element processes, testing and evaluation procedures, delivery mechanisms, support mechanisms, communications/delivery paths, and disposal/final disposition activities as well as the components and tools used, establishes a foundational identity structure for assessment of supply chain activities. For example, labeling (using serial numbers) and tagging (using radio-frequency identification [RFID] tags) individual supply chain elements including software packages, modules, and hardware devices, and processes associated with those elements can be used for this purpose. Identification methods are sufficient to support the provenance in the event of a supply chain issue or adverse supply chain event.

(16) *SUPPLY CHAIN PROTECTION | PROCESSES TO ADDRESS WEAKNESSES OR DEFICIENCIES*

The organization establishes a process to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.

Supplemental Guidance: Evidence generated during independent or organizational assessments of supply chain elements (e.g., penetration testing, audits, verification/validation activities) is documented and used in follow-on processes implemented by organizations to respond to the risks related to the identified weaknesses and deficiencies. Supply chain elements include, for example, supplier development processes and supplier distribution systems.

References: NIST Special Publication 800-161; NIST Interagency Report 7622.

Deleted: None

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** Not Selected	**HIGH** SA-12

SA-13 TRUSTWORTHINESS

Control: The organization:

Deleted: requires that

a. Describes the trustworthiness required in the [*Assignment: organization-defined information system, information system component, or information system service*] supporting its critical missions/business functions; and

b. Implements [*Assignment: organization-defined assurance overlay*] to achieve such trustworthiness.

Supplemental Guidance: This control helps organizations to make explicit trustworthiness decisions when designing, developing, and implementing information systems that are needed to conduct critical organizational missions/business functions. Trustworthiness is a characteristic/property of an information system that expresses the degree to which the system can be expected to preserve the confidentiality, integrity, and availability of the information it processes, stores, or transmits. Trustworthy information systems are systems that are capable of being trusted to operate within defined levels of *risk* despite the environmental disruptions, human errors, and purposeful attacks that are expected to occur in the specified environments of operation. Trustworthy systems are important to mission/business success. Two factors affecting the trustworthiness of information systems include: (i) security functionality (i.e., the security features, functions, and/or mechanisms employed within the system and its environment of operation); and (ii) security assurance (i.e., the grounds for confidence that the security functionality is effective in its application). Developers, implementers, operators, and maintainers of organizational information systems can increase the level of assurance (and trustworthiness), for example, by employing well-defined security policy models, structured and rigorous hardware, software, and firmware development techniques, sound system/security engineering principles, and secure configuration settings (defined by a set of assurance-related security controls in Appendix E).

Assurance is also based on the assessment of evidence produced during the system development life cycle. Critical missions/business functions are supported by high-impact systems and the associated assurance requirements for such systems. The additional assurance controls in Table E-4 in Appendix E (designated as optional) can be used to develop and implement high-assurance solutions for specific information systems and system components using the concept of overlays described in Appendix I. Organizations select assurance overlays that have been developed, validated, and approved for community adoption (e.g., cross-organization, governmentwide), limiting the development of such overlays on an organization-by-organization basis. Organizations can conduct criticality analyses as described in SA-14, to determine the information systems, system components, or information system services that require high-assurance solutions. Trustworthiness requirements and assurance overlays can be described in the security plans for organizational information systems. Related controls: RA-2, SA-4, SA-8, SA-14, SC-3.

Control Enhancements: None.

References: FIPS Publications 199, 200; NIST Special Publications 800-53, 800-53A, 800-60, 800-64.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SA-14 CRITICALITY ANALYSIS

Control: The organization identifies critical information system components and functions by performing a criticality analysis for [*Assignment: organization-defined information systems, information system components, or information system services*] at [*Assignment: organization-defined decision points in the system development life cycle*].

Supplemental Guidance: Criticality analysis is a key tenet of supply chain risk management and informs the prioritization of supply chain protection activities such as attack surface reduction, use of all-source intelligence, and tailored acquisition strategies. Information system engineers can conduct an end-to-end functional decomposition of an information system to identify mission-

Deleted: information system meets

Deleted: *level of trustworthiness*].

Deleted: The intent of this

Deleted: is to ensure that

Deleted: recognize the importance of trustworthiness and making

Deleted: organizational

Deleted: .

Deleted: or

Deleted: being processed, stored, or transmitted by the system.

Deleted: an

Deleted: system

Deleted: or

Deleted: Appropriate security functionality for the information system can be obtained by using the Risk Management Framework (Steps 1, 2, and 3) to select and implement the necessary management, operational, and technical security controls necessary to mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation. Appropriate security assurance can be obtained by: (i) the actions taken by developers and implementers of security controls with regard to the design, development, implementation, and operation of those controls; and (ii) the actions taken by assessors to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system.¶
Developers and implementers can increase the assurance in security controls by employing well-defined security policy models, structured, disciplined, and rigorous hardware and softwar

Deleted: initiation, acquisition/development,

Deleted: For example, developmental evider

Deleted: E. ¶

Deleted: resilience and security capability

Deleted: adjusting the risk management

Deleted: may be defined on a component-by

Deleted: P1

Deleted: SA-13

Deleted: CRITICAL INFORMATION SYSTE

Deleted:

Deleted: :¶

Deleted: *that require re-implementation*];

Deleted: ¶

Deleted: .

Deleted: Supplemental Guidance: The

critical functions and components. The functional decomposition includes the identification of core organizational missions supported by the system, decomposition into the specific functions to perform those missions, and traceability to the hardware, software, and firmware components that implement those functions, including when the functions are shared by many components within and beyond the information system boundary. Information system components that allow for unmediated access to critical components or functions are considered critical due to the inherent vulnerabilities such components create. Criticality is assessed in terms of the impact of the function or component failure on the ability of the component to complete the organizational missions supported by the information system. A criticality analysis is performed whenever an architecture or design is being developed or modified, including upgrades. Related controls: CP-2, PL-2, PL-8, PM-1, SA-8, SA-12, SA-13, SA-15, SA-20.

Control Enhancements: None.

(1) *CRITICALITY ANALYSIS | CRITICAL COMPONENTS WITH NO VIABLE ALTERNATIVE SOURCING*

[Withdrawn: Incorporated into SA-20].

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

Deleted: <#>The organization:¶
<#>Identifies information system components for which alternative sourcing is not viable; and¶
<#>Employs [*Assignment: organization-defined measures*] to ensure that critical security controls for the information system components are not compromised.¶
Enhancement Supplemental Guidance: Measures that the organization considers implementing include, for example, enhanced auditing, restrictions on source code and system utility access, and protection from deletion of system and application files.¶

SA-15 DEVELOPMENT PROCESS, STANDARDS, AND TOOLS

Control: The organization:

a. Requires the developer of the information system, system component, or information system service to follow a documented development process that:

1. Explicitly addresses security requirements;

2. Identifies the standards and tools used in the development process;

3. Documents the specific tool options and tool configurations used in the development process; and

4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and

b. Reviews the development process, standards, tools, and tool options/configurations [*Assignment: organization-defined frequency*] to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy [*Assignment: organization-defined security requirements*].

Supplemental Guidance: Development tools include, for example, programming languages and computer-aided design (CAD) 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 enables accurate supply chain risk assessment and mitigation, and requires robust configuration control throughout the life cycle (including design, development, transport, delivery, integration, and maintenance) to track authorized changes and prevent unauthorized changes. Related controls: SA-3, SA-8.

Control Enhancements:

(1) *DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | QUALITY METRICS*

The organization requires the developer of the information system, system component, or information system service to:

(a) Define quality metrics at the beginning of the development process; and

(b) Provide evidence of meeting the quality metrics [*Selection (one or more):* [*Assignment: organization-defined frequency*]; [*Assignment: organization-defined program review milestones*]; *upon delivery*].

Supplemental Guidance: Organizations use quality metrics to establish minimum acceptable levels of information system quality. Metrics may include quality gates which are collections of completion criteria or sufficiency standards representing the satisfactory execution of particular phases of the system development project. A quality gate, for example, may require the elimination of all compiler warnings or an explicit determination that the warnings have no impact on the effectiveness of required security 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 information system with a Common Vulnerability Scoring System (CVSS) severity of Medium or High.

(2) *DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | SECURITY TRACKING TOOLS*

The organization requires the developer of the information system, system component, or information system service to select and employ a security tracking tool for use during the development process.

Supplemental Guidance: Information 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.

(3) *DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | CRITICALITY ANALYSIS*

The organization requires the developer of the information system, system component, or information system service to perform a criticality analysis at [*Assignment: organization-defined breadth/depth*] and at [*Assignment: organization-defined decision points in the system development life cycle*].

Supplemental Guidance: This control enhancement provides developer input to the criticality analysis performed by organizations in SA-14. Developer input is essential to such analysis because organizations may not have access to detailed design documentation for information system components that are developed as commercial off-the-shelf (COTS) information technology products (e.g., functional specifications, high-level designs, low-level designs, and source code/hardware schematics). Related controls: SA-4, SA-14.

(4) *DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | THREAT MODELING / VULNERABILITY ANALYSIS*

The organization requires that developers perform threat modeling and a vulnerability analysis for the information system at [*Assignment: organization-defined breadth/depth*] that:

(a) Uses [*Assignment: organization-defined information concerning impact, environment of operations, known or assumed threats, and acceptable risk levels*];

(b) Employs [*Assignment: organization-defined tools and methods*]; and

(c) Produces evidence that meets [*Assignment: organization-defined acceptance criteria*].

Supplemental Guidance: Related control: SA-4.

(5) *DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | ATTACK SURFACE REDUCTION*

The organization requires the developer of the information system, system component, or information system service to reduce attack surfaces to [*Assignment: organization-defined thresholds*].

Supplemental Guidance: Attack surface reduction is closely aligned with developer threat and vulnerability analyses and information 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 information systems, information system components, and information system services. Attack surface reduction includes, for example, applying the principle of least privilege, employing layered defenses, applying the principle of least functionality (i.e., restricting ports, protocols, functions, and services), deprecating unsafe functions, and eliminating application programming interfaces (APIs) that are vulnerable to cyber attacks. Related control: CM-7.

(6) *DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | CONTINUOUS IMPROVEMENT*

The organization requires the developer of the information system, system component, or information system service to implement an explicit process to continuously improve the development process.

Supplemental Guidance: Developers of information systems, information system components, and information system services consider the effectiveness/efficiency of current development processes for meeting quality objectives and addressing security capabilities in current threat environments.

(7) *DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | AUTOMATED VULNERABILITY ANALYSIS*

The organization requires the developer of the information system, system component, or information system service to:

(a) Perform an automated vulnerability analysis using [*Assignment: organization-defined tools*];

(b) Determine the exploitation potential for discovered vulnerabilities;

(c) Determine potential risk mitigations for delivered vulnerabilities; and

(d) Deliver the outputs of the tools and results of the analysis to [*Assignment: organization-defined personnel or roles*].

Supplemental Guidance: Related control: RA-5.

(8) *DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | REUSE OF THREAT / VULNERABILITY INFORMATION*

The organization requires the developer of the information system, system component, or information system service to use threat modeling and vulnerability analyses from similar systems, components, or services to inform the current development process.

Supplemental Guidance: Analysis of vulnerabilities found in similar software applications can inform potential design or implementation issues for information systems under development. Similar information systems or system components may exist within developer organizations. Authoritative vulnerability information is available from a variety of public and private sector sources including, for example, the National Vulnerability Database.

(9) *DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | USE OF LIVE DATA*

The organization approves, documents, and controls the use of live data in development and test environments for the information system, system component, or information system service.

Supplemental Guidance: The use of live data in preproduction environments can result in significant risk to organizations. Organizations can minimize such risk by using test or dummy data during the development and testing of information systems, information system components, and information system services.

(10) *DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | INCIDENT RESPONSE PLAN*

The organization requires the developer of the information system, system component, or information system service to provide an incident response plan.

Supplemental Guidance: The incident response plan for developers of information systems, system components, and information system services is incorporated into organizational incident response plans to provide the type of incident response information not readily available to organizations. Such information may be extremely helpful, for example, when organizations respond to vulnerabilities in commercial off-the-shelf (COTS) information technology products. Related control: IR-8.

(11) *DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | ARCHIVE INFORMATION SYSTEM / COMPONENT*

The organization requires the developer of the information system or system component to archive the system or component to be released or delivered together with the corresponding evidence supporting the final security review.

Supplemental Guidance: Archiving relevant documentation from the development process can provide a readily available baseline of information that can be helpful during information system/component upgrades or modifications.

References: None.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** Not Selected	**HIGH** SA-15

SA-16 DEVELOPER-PROVIDED TRAINING

Control: The organization requires the developer of the information system, system component, or information system service to provide [*Assignment: organization-defined training*] on the correct use and operation of the implemented security functions, controls, and/or mechanisms.

Supplemental Guidance: This control applies to external and internal (in-house) developers. Training of personnel is an essential element to ensure the effectiveness of security controls implemented within organizational information systems. Training options include, for example, classroom-style training, web-based/computer-based training, and hands-on training. Organizations can also request sufficient 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 functions, controls, or mechanisms. Related controls: AT-2, AT-3, SA-5.

References: None.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** Not Selected	**HIGH** SA-16

SA-17 DEVELOPER SECURITY ARCHITECTURE AND DESIGN

Control: The organization requires the developer of the information system, system component, or information system service to produce a design specification and security architecture that:

a. Is consistent with and supportive of the organization’s security architecture which is established within and is an integrated part of the organization’s enterprise architecture;

b. Accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components; and

c. Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection.

Supplemental Guidance: This control is primarily directed at external developers, although it could also be used for internal (in-house) development. In contrast, PL-8 is primarily directed at internal developers to help ensure that organizations develop an information security architecture and such security architecture is integrated or tightly coupled to the enterprise architecture. This distinction is important if/when organizations outsource the development of information systems, information system components, or information system services to external entities, and there is a requirement to demonstrate consistency with the organization’s enterprise architecture and information security architecture. Related controls: PL-8, PM-7, SA-3, SA-8.

Control Enhancements:

(1) *DEVELOPER SECURITY ARCHITECTURE AND DESIGN | FORMAL POLICY MODEL*

The organization requires the developer of the information system, system component, or information system service to:

(a) Produce, as an integral part of the development process, a formal policy model describing the [*Assignment: organization-defined elements of organizational security policy*] to be enforced; and

(b) Prove that the formal policy model is internally consistent and sufficient to enforce the defined elements of the organizational security policy when implemented.

Supplemental Guidance: Formal models describe specific behaviors or security policies using formal languages, thus enabling the correctness of those behaviors/policies to be formally proven. Not all components of information systems can be modeled, and generally, formal specifications are scoped to specific behaviors or policies of interest (e.g., nondiscretionary access control policies). Organizations choose the particular formal modeling language and approach based on the nature of the behaviors/policies to be described and the available tools. Formal modeling tools include, for example, Gypsy and Zed.

(2) *DEVELOPER SECURITY ARCHITECTURE AND DESIGN | SECURITY-RELEVANT COMPONENTS*

The organization requires the developer of the information system, system component, or information system service to:

(a) Define security-relevant hardware, software, and firmware; and

(b) Provide a rationale that the definition for security-relevant hardware, software, and firmware is complete.

Supplemental Guidance: Security-relevant hardware, software, and firmware represent the portion of the information system, component, or service that must be trusted to perform correctly in order to maintain required security properties. Related control: SA-5.

(3) *DEVELOPER SECURITY ARCHITECTURE AND DESIGN | FORMAL CORRESPONDENCE*

The organization requires the developer of the information system, system component, or information system service to:

(a) Produce, as an integral part of the development process, a formal top-level specification that specifies the interfaces to security-relevant hardware, software, and firmware in terms of exceptions, error messages, and effects;

(b) Show via proof to the extent feasible with additional informal demonstration as necessary, that the formal top-level specification is consistent with the formal policy model;

(c) Show via informal demonstration, that the formal top-level specification completely covers the interfaces to security-relevant hardware, software, and firmware;

(d) Show that the formal top-level specification is an accurate description of the implemented security-relevant hardware, software, and firmware; and

(e) Describe the security-relevant hardware, software, and firmware mechanisms not addressed in the formal top-level specification but strictly internal to the security-relevant hardware, software, and firmware.

Supplemental Guidance: Correspondence is an important part of the assurance gained through modeling. It demonstrates that the implementation is an accurate transformation of the model, and that any additional code or implementation details 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 information 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/informal methods may be needed to show such consistency. Consistency between the formal top-level specification and the 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/output. Related control: SA-5.

(4) *DEVELOPER SECURITY ARCHITECTURE AND DESIGN | INFORMAL CORRESPONDENCE*

The organization requires the developer of the information system, system component, or information system service to:

(a) Produce, as an integral part of the development process, an informal descriptive top-level specification that specifies the interfaces to security-relevant hardware, software, and firmware in terms of exceptions, error messages, and effects;

(b) Show via [*Selection: informal demonstration, convincing argument with formal methods as feasible*] that the descriptive top-level specification is consistent with the formal policy model;

(c) Show via informal demonstration, that the descriptive top-level specification completely covers the interfaces to security-relevant hardware, software, and firmware;

(d) Show that the descriptive top-level specification is an accurate description of the interfaces to security-relevant hardware, software, and firmware; and

(e) Describe the security-relevant hardware, software, and firmware mechanisms not addressed in the descriptive top-level specification but strictly internal to the security-relevant hardware, software, and firmware.

Supplemental Guidance: Correspondence is an important part of the assurance gained through modeling. It demonstrates that the implementation is an accurate transformation of the model, and that any additional code or implementation details present has no impact on the behaviors or policies being modeled. Consistency between the descriptive top-level specification (i.e., high-level/low-level design) and the formal policy model is generally not amenable to being fully proven. Therefore, a combination of formal/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/output. Related control: SA-5.

(5) *DEVELOPER SECURITY ARCHITECTURE AND DESIGN | CONCEPTUALLY SIMPLE DESIGN*

The organization requires the developer of the information system, system component, or information system service to:

(a) Design and structure the security-relevant hardware, software, and firmware to use a complete, conceptually simple protection mechanism with precisely defined semantics; and

(b) Internally structure the security-relevant hardware, software, and firmware with specific regard for this mechanism.

Supplemental Guidance: Related control: SC-3.

(6) *DEVELOPER SECURITY ARCHITECTURE AND DESIGN | STRUCTURE FOR TESTING*

The organization requires the developer of the information system, system component, or information system service to structure security-relevant hardware, software, and firmware to facilitate testing.

Supplemental Guidance: Related control: SA-11.

(7) *DEVELOPER SECURITY ARCHITECTURE AND DESIGN | STRUCTURE FOR LEAST PRIVILEGE*

The organization requires the developer of the information system, system component, or information system service to structure security-relevant hardware, software, and firmware to facilitate controlling access with least privilege.

Supplemental Guidance: Related controls: AC-5, AC-6.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** Not Selected	**HIGH** SA-17

SA-18 TAMPER RESISTANCE AND DETECTION

Control: The organization implements a tamper protection program for the information system, system component, or information system service.

Supplemental Guidance: Anti-tamper technologies and techniques provide a level of protection for critical information systems, system components, and information technology products against a number of related threats including modification, reverse engineering, and substitution. Strong identification combined with tamper resistance and/or tamper detection is essential to protecting information systems, components, and products during distribution and when in use. Related controls: PE-3, SA-12, SI-7.

Control Enhancements:

(1) *TAMPER RESISTANCE AND DETECTION | MULTIPLE PHASES OF SDLC*

The organization employs anti-tamper technologies and techniques during multiple phases in the system development life cycle including design, development, integration, operations, and maintenance.

Supplemental Guidance: Organizations use a combination of hardware and software techniques for tamper resistance and detection. Organizations employ obfuscation and self-checking, for example, to make reverse engineering and modifications more difficult, time-consuming, and expensive for adversaries. Customization of information systems and system components can make substitutions easier to detect and therefore limit damage. Related control: SA-3.

(2) *TAMPER RESISTANCE AND DETECTION | INSPECTION OF INFORMATION SYSTEMS, COMPONENTS, OR DEVICES*

The organization inspects [*Assignment: organization-defined information systems, system components, or devices*] [*Selection (one or more): at random;* at [*Assignment: organization-defined frequency*], *upon* [*Assignment: organization-defined indications of need for inspection*]] to detect tampering.

Supplemental Guidance: This control enhancement addresses both 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 need for inspection include, for example, when individuals return from travel to high-risk locations. Related control: SI-4.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SA-19 COMPONENT AUTHENTICITY

Control: The organization:

a. Develops and implements anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the information system; and

b. Reports counterfeit information system components to [*Selection (one or more): source of counterfeit component;* [*Assignment: organization-defined external reporting organizations*]; [*Assignment: organization-defined personnel or roles*]].

Supplemental Guidance: Sources of counterfeit components include, for example, manufacturers, developers, vendors, and contractors. Anti-counterfeiting policy and procedures support tamper resistance and provide a level of protection against the introduction of malicious code. External reporting organizations include, for example, US-CERT. Related controls: PE-3, SA-12, SI-7.

Control Enhancements:

(1) *COMPONENT AUTHENTICITY | ANTI-COUNTERFEIT TRAINING*

The organization trains [*Assignment: organization-defined personnel or roles*] to detect counterfeit information system components (including hardware, software, and firmware).

(2) *COMPONENT AUTHENTICITY | CONFIGURATION CONTROL FOR COMPONENT SERVICE / REPAIR*

The organization maintains configuration control over [*Assignment: organization-defined information system components*] awaiting service/repair and serviced/repaired components awaiting return to service.

(3) *COMPONENT AUTHENTICITY | COMPONENT DISPOSAL*

The organization disposes of information system components using [*Assignment: organization-defined techniques and methods*].

Supplemental Guidance: Proper disposal of information system components helps to prevent such components from entering the gray market.

(4) *COMPONENT AUTHENTICITY | ANTI-COUNTERFEIT TRAINING*

The organization scans for counterfeit information system components [*Assignment: organization-defined frequency*].

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SA-20 CUSTOMIZED DEVELOPMENT OF CRITICAL COMPONENTS

Control: The organization re-implements or custom develops [*Assignment: organization-defined critical information system components*].

Supplemental Guidance: Organizations determine that certain information 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 information system components, additional safeguards can be employed (e.g., enhanced auditing, restrictions on source code and system utility access, and protection from deletion of system and application files. Related controls: CP-2, SA-8, SA-14.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SA-21 DEVELOPER SCREENING

Control: The organization requires that the developer of [*Assignment: organization-defined information system, system component, or information system service*]:

a. Have appropriate access authorizations as determined by assigned [*Assignment: organization-defined official government duties*]; and

b. Satisfy [*Assignment: organization-defined additional personnel screening criteria*].

Supplemental Guidance: Because the information system, system component, or information system service may be employed in critical activities essential to the national and/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 information system/component/service once deployed. Examples of authorization and personnel screening criteria include clearance, satisfactory 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/reliability of the systems, components, or services being developed. Related controls: PS-3, PS-7.

Control Enhancements:

(1) *DEVELOPER SCREENING | VALIDATION OF SCREENING*

The organization requires the developer of the information system, system component, or information system service take [*Assignment: organization-defined actions*] to ensure that the required access authorizations and screening criteria are satisfied.

Supplemental Guidance: Satisfying required access authorizations and personnel screening criteria includes, for example, providing a listing of all the individuals authorized to perform development activities on the selected information system, system component, or information system service so that organizations can validate that the developer has satisfied the necessary authorization and screening requirements.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SA-22 UNSUPPORTED SYSTEM COMPONENTS

Control: The organization:

a. Replaces information system components when support for the components is no longer available from the developer, vendor, or manufacturer; and

b. Provides justification and documents approval for the continued use of unsupported system components required to satisfy mission/business needs.

Supplemental Guidance: Support for information system components includes, for example, software patches, firmware updates, replacement parts, and maintenance contracts. Unsupported components (e.g., when vendors are no longer providing critical software patches), provide a substantial opportunity for adversaries to exploit new weaknesses discovered in the currently installed components. Exceptions to replacing unsupported system components may include, for example, systems that provide critical mission/business capability where newer technologies are not available or where the systems are so isolated that installing replacement components is not an option. Related controls: PL-2, SA-3.

Control Enhancements:

(1) *UNSUPPORTED SYSTEM COMPONENTS | ALTERNATIVE SOURCES FOR CONTINUED SUPPORT*

The organization provides [*Selection (one or more): in-house support; [Assignment: organization-defined support from external providers*]] for unsupported information system components.

Supplemental Guidance: This control enhancement addresses the need to provide continued support for selected information system components that are no longer supported by the original developers, vendors, or manufacturers when such components remain essential to mission/business operations. Organizations can establish in-house support, for example, by developing customized patches for critical software components or secure 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.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

Formatted: Font: (Default) Arial, 8 pt, Bold

SYSTEM AND SERVICES ACQUISITION CONTROLS

DEVELOPMENT OF SYSTEMS, COMPONENTS, AND SERVICES

With the renewed emphasis on trustworthy information systems and supply chain security, it is essential that organizations have the capability to express their information security requirements with clarity and specificity in order to engage the information technology industry and obtain the systems, components, and services necessary for mission and business success. To ensure that organizations have such capability, this publication provides a set of security controls in the System and Services Acquisition family (i.e., SA family) addressing requirements for the development of information systems, information technology products, and information system services. Therefore, many of the controls in the SA family are directed at developers of those systems, components, and services. It is important for organizations to recognize that the scope of the security controls in the SA family includes all system/component/service development and the developers associated with

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION

SC-1 SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and

b. Reviews and updates the current:

1. System and communications protection policy [*Assignment: organization-defined frequency*]; and

2. System and communications protection procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the SC family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

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

Priority and Baseline Allocation:

P1	**LOW** SC-1	**MOD** SC-1	**HIGH** SC-1

SC-2 APPLICATION PARTITIONING

Control: The information system separates user functionality (including user interface services) from information system management functionality.

Supplemental Guidance: Information system management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access. The separation of user functionality from information system management functionality is either physical or logical. Organizations implement separation of system management-related functionality from user functionality by using different computers, different central processing units, different instances of operating systems, different network addresses, virtualization techniques, or combinations of these or other methods, as appropriate. This type of separation includes, for example, web administrative interfaces that use separate authentication methods for users of any other information system resources. Separation of system and user functionality may include isolating administrative interfaces on different domains and with additional access controls. Related controls: SA-4, SA-8, SC-3.

Control Enhancements:

Deleted: CLASS: TECHNICAL

Deleted: develops,

Deleted: , and reviews/updates

Deleted: *frequency*

Deleted: A formal, documented

Deleted: Formal, documented procedures

Deleted: .

Deleted: is intended to produce

Deleted: that are required

Deleted: system and communications protection

Deleted: The policy

Deleted: are consistent with

Deleted: policies,

Deleted: Existing organizational

Deleted: additional

Deleted:

Deleted: system and communications protection

Deleted: the organization. System and communications protection

Deleted: developed

Deleted: a

Deleted: system, when required.

Deleted: the development of the system and communications protection

Deleted: .

Deleted:

Deleted: and is accomplished

Deleted: the

Deleted: system

Deleted: methods,

Deleted: An example of this

Deleted: is observed in

Deleted: This

Deleted: the

Deleted: interface

Deleted: a

Deleted: domain

(1) *APPLICATION PARTITIONING | INTERFACES FOR NON-PRIVILEGED USERS*

The information system prevents the presentation of information system management-related functionality at an interface for non-privileged users.

Supplemental Guidance: This control enhancement ensures that administration options (e.g., administrator privileges) are not available to general users (including prohibiting the use of the grey-out option commonly used to eliminate accessibility to such information). Such restrictions include, for example, not presenting administration options until users establish sessions with administrator privileges. Related control: AC-3.

Deleted: general (i.e.,

Deleted:)

Deleted: Enhancement

Deleted: The intent of this

Deleted: is to ensure

Deleted: For

Deleted: are not presented

Deleted: the user has appropriately established a session

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SC-2	**HIGH** SC-2

SC-3 SECURITY FUNCTION ISOLATION

Control: The information system isolates security functions from nonsecurity functions.

Supplemental Guidance: The information 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. Information systems implement code separation (i.e., separation of security functions from nonsecurity functions) in a number of ways, including, 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 serve to protect the code on disk, and address space protections that protect executing code. Information systems restrict access to security functions through the use of access control mechanisms and by implementing least privilege capabilities. While the ideal is for all of the code within the security function isolation boundary to only contain security-relevant code, it is sometimes necessary to include nonsecurity functions within the isolation boundary as an exception. Related controls: AC-3, AC-6, SA-4, SA-5, SA-8, SA-13, SC-2, SC-7, SC-39.

Deleted:) that

Deleted: ,

Deleted: The information

Deleted: maintains a separate execution domain (e.g.,

Deleted:) for each

Deleted: process.

Deleted: control:

Control Enhancements:

(1) *SECURITY FUNCTION ISOLATION | HARDWARE SEPARATION*

The information system utilizes underlying hardware separation mechanisms to implement security function isolation.

Deleted: implements

Deleted: facilitate

Supplemental Guidance: Underlying hardware separation mechanisms include, for example, hardware ring architectures, commonly implemented within microprocessors, and hardware-enforced address segmentation used to support logically distinct storage objects with separate attributes (i.e., readable, writeable).

(2) *SECURITY FUNCTION ISOLATION | ACCESS / FLOW CONTROL FUNCTIONS*

The information system isolates security functions enforcing access and information flow control from nonsecurity functions and from other security functions.

Deleted: both

Supplemental Guidance: Security function isolation occurs as a result 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.

(3) *SECURITY FUNCTION ISOLATION | MINIMIZE NONSECURITY FUNCTIONALITY*

The organization minimizes the number of nonsecurity functions included within the isolation boundary containing security functions.

Deleted: implements an information system isolation boundary to minimize

Supplemental Guidance: In those instances where it is not feasible to achieve strict isolation of nonsecurity functions from security functions, it is necessary to take actions to minimize the nonsecurity-relevant functions within the security function boundary. Nonsecurity functions contained within the isolation boundary are considered security-relevant because errors or

Deleted: Enhancement Supplemental Guidance:

Deleted: .

maliciousness in such software, by virtue of being within the boundary, can impact the security functions of organizational information systems. The design objective is that the specific portions of information systems providing information security are of minimal size/complexity. Minimizing the number of nonsecurity functions in the security-relevant components of information systems 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 reduced, thus contributing to understandability.

(4) *SECURITY FUNCTION ISOLATION | MODULE COUPLING AND COHESIVENESS*

The organization implements security functions as largely independent modules that maximize internal cohesiveness within modules and minimize coupling between modules.

Supplemental Guidance: The reduction in inter-module interactions helps to constrain security functions and to manage complexity. The concepts of coupling and cohesion are important with respect to modularity in software design. Coupling refers to the dependencies that one module has on other modules. Cohesion refers to the relationship between the different functions within a particular module. Good software engineering practices rely on modular decomposition, layering, and minimization to reduce and manage complexity, thus producing software modules that are highly cohesive and loosely coupled.

(5) *SECURITY FUNCTION ISOLATION | LAYERED STRUCTURES*

The organization implements security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.

Supplemental Guidance: The implementation of layered structures with minimized interactions among security functions and non-looping layers (i.e., lower-layer functions do not depend on higher-layer functions) further enables the isolation of security functions and management of complexity.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** Not Selected	**HIGH** SC-3

SC-4 INFORMATION IN SHARED RESOURCES

Control: The information system prevents unauthorized and unintended information transfer via shared system resources.

Supplemental Guidance: This control prevents information, including encrypted representations of information, produced by the actions of prior users/roles (or the actions of processes acting on behalf of prior users/roles) from being available to any current users/roles (or current processes) that obtain access to shared system resources (e.g., registers, main memory, hard disks) after those resources have been released back to information systems. The control of information in shared resources is also commonly referred to as object reuse and residual information protection. This control does not address: (i) information remanence which refers to residual representation of data that has been nominally erased or removed; (ii) covert channels (including storage and/or timing channels) where shared resources are manipulated to violate information flow restrictions; or (iii) components within information systems for which there are only single users/roles. Related controls: AC-3, AC-4, MP-6.

Control Enhancements:

(1) *INFORMATION IN SHARED RESOURCES | SECURITY LEVELS*

[Withdrawn: Incorporated into SC-4].

(2) *INFORMATION IN SHARED RESOURCES | PERIODS PROCESSING*

Deleted: avoid unnecessary interactions

Deleted: The purpose of this

Deleted: is to prevent

Deleted: a

Deleted: user/role

Deleted: a process

Deleted: a

Deleted: user/role

Deleted: user/role

Deleted: process

Deleted: obtains

Deleted: a

Deleted: resource

Deleted: secondary storage

Deleted: that resource has

Deleted: the

Deleted: system. Control

Deleted: .

Deleted: in some way

Deleted: achieve a violation of

Deleted: in the

Deleted: system

Deleted: is

Deleted: a

Deleted: user/role

Deleted: <#>The information system does not share resources that are used to interface with systems operating at different security levels.¶
Enhancement Supplemental Guidance: Shared resources include, for example, memory, input/output queues, and network interface cards.¶

The information system prevents unauthorized information transfer via shared resources in accordance with [*Assignment: organization-defined procedures*] when system processing explicitly switches between different information classification levels or security categories.

Supplemental Guidance: This control enhancement applies when there are explicit changes in information processing levels during information system operations, for example, during multilevel processing and 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.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SC-4	**HIGH** SC-4

SC-5 DENIAL OF SERVICE PROTECTION

Control: The information system protects against or limits the effects of the following types of denial of service attacks: [*Assignment: organization-defined types of denial of service attacks or reference to source for such information*] by employing [*Assignment: organization-defined security safeguards*].

Deleted: *list of*

Deleted: *current list*

Supplemental Guidance: A variety of technologies exist to limit, or in some cases, eliminate the effects of denial of service attacks. For example, boundary protection devices can filter certain types of packets to protect information system components on internal organizational networks from being directly affected by denial of service attacks. Employing increased capacity and bandwidth combined with service redundancy may also reduce the susceptibility to denial of service attacks. Related controls: SC-6, SC-7.

Deleted:

Deleted: devices

Deleted: an organization's

Deleted: network

Deleted:

Deleted: some

Deleted:

Deleted: control

Control Enhancements:

(1) *DENIAL OF SERVICE PROTECTION | RESTRICT INTERNAL USERS*

The information system restricts the ability of individuals to launch [*Assignment: organization-defined denial of service attacks*] against other information systems.

Deleted: users

Deleted: or **networks**

Supplemental Guidance: Restricting the ability of individuals to launch denial of service attacks requires that the mechanisms used for such attacks are unavailable. Individuals of concern can include, for example, hostile insiders or external adversaries that have successfully breached the information system and are using the system as a platform to launch cyber attacks on third parties. Organizations can restrict the ability of individuals to connect and transmit arbitrary information on the transport medium (i.e., network, wireless spectrum). Organizations can also limit the ability of individuals to use excessive information system resources. Protection against individuals having the ability to launch denial of service attacks may be implemented on specific information systems or on boundary devices prohibiting egress to potential target systems.

(2) *DENIAL OF SERVICE PROTECTION | EXCESS CAPACITY / BANDWIDTH / REDUNDANCY*

The information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding denial of service attacks.

Deleted: types of

Supplemental Guidance: Managing excess capacity ensures that sufficient capacity is available to counter flooding attacks. Managing excess capacity may include, for example, establishing selected usage priorities, quotas, or partitioning.

(3) *DENIAL OF SERVICE PROTECTION | DETECTION / MONITORING*

The organization:

(a) Employs [*Assignment: organization-defined monitoring tools*] to detect indicators of denial of service attacks against the information system; and

(b) Monitors [*Assignment: organization-defined information system resources*] to determine if sufficient resources exist to prevent effective denial of service attacks.

Supplemental Guidance: Organizations consider utilization and capacity of information system resources when managing risk from denial of service due to malicious attacks. Denial of service attacks can originate from external or internal sources. Information system resources sensitive to denial of service include, for example, physical disk storage, memory, and CPU cycles. Common safeguards to prevent denial of service attacks related to storage utilization and capacity include, for example, instituting disk quotas, configuring information systems to automatically alert administrators when specific storage capacity thresholds are reached, using file compression technologies to maximize available storage space, and imposing separate partitions for system and user data. Related controls: CA-7, SI-4.

References: None.

Priority and Baseline Allocation:

P1	**LOW** SC-5	**MOD** SC-5	**HIGH** SC-5

SC-6 RESOURCE AVAILABILITY

Control: The information system protects the availability of resources by allocating [*Assignment: organization-defined resources*] by [*Selection (one or more); priority; quota;* [*Assignment: organization-defined security safeguards*]].

Supplemental Guidance: Priority protection helps prevent lower-priority processes from delaying or interfering with the information system servicing any higher-priority processes. Quotas prevent users or processes from obtaining more than predetermined amounts of resources. This control does not apply to information system components for which there are only single users/roles.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

Deleted: PRIORITY

Deleted: limits

Deleted: use

Deleted: .

Deleted: a

Deleted: process

Deleted: process.

Deleted: components in the

Deleted: is

Deleted: a

Deleted: user/role

SC-7 BOUNDARY PROTECTION

Control: The information system:

a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system;

b. Implements subnetworks for publicly accessible system components that are [*Selection: physically; logically*] separated from internal organizational networks; and

c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

Supplemental Guidance: Managed interfaces include, for example, gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within a security architecture (e.g., routers protecting firewalls or application gateways residing on protected subnetworks). Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones or DMZs. Restricting or prohibiting interfaces within organizational information systems includes, for example, restricting external web traffic to designated web servers within managed interfaces and prohibiting external traffic that appears to be spoofing internal addresses. Organizations consider the shared nature of commercial telecommunications services in the implementation of security controls associated

Deleted: and

Deleted: Restricting external web traffic only to organizational web servers within managed interfaces and prohibiting external traffic that appears to be spoofing an internal address as the source are examples of restricting and prohibiting communications.

Deleted: employing boundary protection devices

Deleted: proxies,

Deleted: arranged in an effective

Deleted: and

Deleted: a

Deleted: subnetwork commonly referred to as a demilitarized zone or DMZ).¶
The organization considers the intrinsically

with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may also include third party-provided access lines and other service elements. Such transmission services may represent sources of increased risk despite contract security provisions. Related controls: AC-4, AC-17, CA-3, CM-7, CP-8, IR-4, RA-3, SC-5, SC-13.

Control Enhancements:

(1) *BOUNDARY PROTECTION | PHYSICALLY SEPARATED SUBNETWORKS*

[Withdrawn: Incorporated into SC-7].

(2) *BOUNDARY PROTECTION | PUBLIC ACCESS*

[Withdrawn: Incorporated into SC-7].

(3) *BOUNDARY PROTECTION | ACCESS POINTS*

The organization limits the number of external network connections to the information system.

Supplemental Guidance: Limiting the number of external network connections facilitates more comprehensive monitoring of inbound and outbound communications traffic. The Trusted Internet Connection (TIC) initiative is an example of limiting the number of external network connections.

(4) *BOUNDARY PROTECTION | EXTERNAL TELECOMMUNICATIONS SERVICES*

The organization:

(a) Implements a managed interface for each external telecommunication service;

(b) Establishes a traffic flow policy for each managed interface;

(c) Protects the confidentiality and integrity of the information being transmitted across each interface;

(d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and

(e) Reviews exceptions to the traffic flow policy [*Assignment: organization-defined frequency*] and removes exceptions that are no longer supported by an explicit mission/business need.

Supplemental Guidance: Related control: SC-8.

(5) *BOUNDARY PROTECTION | DENY BY DEFAULT / ALLOW BY EXCEPTION*

The information system at managed interfaces denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception).

Supplemental Guidance: This control enhancement applies to both inbound and outbound network communications traffic. A deny-all, permit-by-exception network communications traffic policy ensures that only those connections which are essential and approved are allowed.

(6) *BOUNDARY PROTECTION | RESPONSE TO RECOGNIZED FAILURES*

[Withdrawn: Incorporated into SC-7 (18)].

(7) *BOUNDARY PROTECTION | PREVENT SPLIT TUNNELING FOR REMOTE DEVICES*

The information system, in conjunction with a remote device, prevents the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks.

Supplemental Guidance: This control enhancement is implemented within remote devices (e.g., 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 information 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 information system resources such as printers/file servers. However, split tunneling would in effect 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 appropriate security controls, may provide the organization with sufficient assurance that it

Deleted:

Deleted: -

Deleted:

Deleted: Consequently, such interconnecting

Deleted: Therefore, when this situation occurs, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk.

Deleted: The organization

Deleted: allocates publicly accessible information system components to separate

Deleted: with separate physical network interfaces.

Deleted: Enhancement Supplemental Guidance: Publicly accessible information ...

Deleted: <#>The information system ...

Deleted: access points

Deleted: to allow for

Deleted: and network

Deleted: ¶ ...

Deleted: managed

Deleted: access points

Deleted: Employs security controls a ...

Deleted:];

Deleted: ¶ ...

Deleted: ,

Deleted: remote devices that have ...

Deleted: connection

Deleted: from

Deleted: outside of that communicatio ...

Deleted: Enhancement

Deleted: the

Deleted: device

Deleted: /laptop computer) via

Deleted: that are not configurable by the us ...

Deleted: prevent *split-tunneling*.

Deleted: otherwise

Deleted: used

Deleted: the information system as an ...

Deleted: a printer or

Deleted: server. Since the remote device, ...

Deleted: be,

Deleted: , allowing

Deleted: into the system

can effectively treat such connections as non-remote connections from the confidentiality and integrity perspective. VPNs thus 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.

(8) *BOUNDARY PROTECTION | ROUTE TRAFFIC TO AUTHENTICATED PROXY SERVERS*

The information system routes [*Assignment: organization-defined internal communications traffic*] to [*Assignment: organization-defined external networks*] through authenticated proxy servers at managed interfaces.

Supplemental Guidance: External networks are networks outside of organizational control. A proxy server is a server (i.e., information system or application) that acts as an intermediary for clients requesting information system resources (e.g., files, connections, web pages, or services) from other organizational servers. Client requests established through an initial connection to the proxy server are evaluated to manage complexity and to provide additional protection by limiting direct connectivity. Web content filtering devices are one of the most common proxy servers providing access to the Internet. Proxy servers support logging individual Transmission Control Protocol (TCP) sessions and blocking specific Uniform Resource Locators (URLs), domain names, and Internet Protocol (IP) addresses. Web proxies can be configured with organization-defined lists of authorized and unauthorized websites. Related controls: AC-3, AU-2.

(9) *BOUNDARY PROTECTION | RESTRICT THREATENING OUTGOING COMMUNICATIONS TRAFFIC*

The information system:

(a) Detects and denies outgoing communications traffic posing a threat to external information systems; and

(b) Audits the identity of internal users associated with denied communications.

Supplemental Guidance: Detecting outgoing communications traffic from internal actions that may pose threats to external information systems is sometimes termed extrusion detection. Extrusion detection at information system boundaries as part of managed interfaces includes the analysis of incoming and outgoing communications traffic searching for indications of internal threats to the security of external systems. Such threats include, for example, traffic indicative of denial of service attacks and traffic containing malicious code. Related controls: AU-2, AU-6, SC-38, SC-44, SI-3, SI-4.

(10) *BOUNDARY PROTECTION | PREVENT UNAUTHORIZED EXFILTRATION*

The organization prevents the unauthorized exfiltration of information across managed interfaces.

Supplemental Guidance: Safeguards implemented by organizations to prevent unauthorized exfiltration of information from information systems include, for example: (i) strict adherence to protocol formats; (ii) monitoring for beaconing from information systems; (iii) monitoring for steganography; (iv) disconnecting external network interfaces except when explicitly needed; (v) disassembling and reassembling packet headers; and (vi) employing traffic profile analysis to detect deviations from the volume/types of traffic expected within organizations or call backs to command and control centers. Devices enforcing strict adherence to protocol formats include, for example, deep packet inspection firewalls and XML gateways. These devices verify adherence to protocol formats and specification at the application layer and serve to identify vulnerabilities that cannot be detected by devices operating at the network or transport layers. This control enhancement is closely associated with cross-domain solutions and system guards enforcing information flow requirements. Related control: SI-3.

(11) *BOUNDARY PROTECTION | RESTRICT INCOMING COMMUNICATIONS TRAFFIC*

The information system only allows incoming communications from [*Assignment: organization-defined authorized sources*] routed to [*Assignment: organization-defined authorized destinations*].

Supplemental Guidance: This control enhancement provides determinations that source and destination address pairs represent authorized/allowed communications. Such determinations can be based on several factors including, for example, the presence of source/destination address pairs in lists of authorized/allowed communications, the absence of address pairs in lists of unauthorized/disallowed pairs, or meeting more general rules for authorized/allowed source/destination pairs. Related control: AC-3.

Deleted: within the

Deleted: of boundary protection devices

Deleted: Enhancement Supplemental Guidance: External networks are networks outside the control of the organization.

Deleted: Proxy servers are also configurable

Deleted: , at managed interfaces,

Deleted: network

Deleted: and audits internal users (or malicious code)

Deleted: .

Deleted: Enhancement

Deleted: a security threat

Deleted:

Deleted: the

Deleted: boundary

Deleted: network traffic (

Deleted: as well as

Deleted:) looking

Deleted: an

Deleted: threat

Deleted: Enhancement

Deleted: Measures

Deleted: the

Deleted: system

Deleted: indications of

Deleted: the

Deleted: system

Deleted: use of

Deleted: or

Deleted: the organization. Examples of devices

Deleted:

Deleted: the

Deleted: layer

Deleted: checks

Deleted: to ensure that the

Deleted: are coming

Deleted: an

(12) *BOUNDARY PROTECTION | HOST-BASED PROTECTION*

The organization implements [*Assignment: organization-defined host-based boundary protection mechanisms*] at [*Assignment: organization-defined information system components*].

Deleted: information …

Supplemental Guidance: Host-based boundary protection mechanisms include, for example, host-based firewalls. Information system components employing host-based boundary protection mechanisms include, for example, servers, workstations, and mobile devices.

(13) *BOUNDARY PROTECTION | ISOLATION OF SECURITY TOOLS / MECHANISMS / SUPPORT COMPONENTS*

The organization isolates [*Assignment: organization-defined information security tools, mechanisms, and support components*] from other internal information system components by implementing physically separate subnetworks with managed interfaces to other components of the system.

Deleted: Enhancement Supplemental Guidance: A host-based boundary protection mechanism is, for example, a host-based firewall. Host-based boundary protection mechanisms are employed on mobile devices, such as notebook/laptop computers, and other types of mobile devices where such boundary protection mechanisms are available.¶

Deleted: *…defined key…information* …

Supplemental Guidance: Physically separate subnetworks with managed interfaces are useful, for example, in isolating computer network defenses from critical operational processing networks to prevent adversaries from discovering the analysis and forensics techniques of organizations. Related controls: SA-8, SC-2, SC-3.

(14) *BOUNDARY PROTECTION | PROTECTS AGAINST UNAUTHORIZED PHYSICAL CONNECTIONS*

The organization protects against unauthorized physical connections at [*Assignment: organization-defined managed interfaces*].

Deleted: across the boundary protections implemented …t …

Deleted: Enhancement …upplemental …

Supplemental Guidance: Information systems operating at different security categories or classification levels may share common physical and environmental controls, since the systems may share space within organizational facilities. In practice, it is possible that these separate information systems may share common equipment rooms, wiring closets, and cable distribution paths. Protection against unauthorized physical connections can be achieved, for example, by employing clearly identified and physically separated cable trays, connection frames, and patch panels for each side of managed interfaces with physical access controls enforcing limited authorized access to these items. Related controls: PE-4, PE-19.

(15) *BOUNDARY PROTECTION | ROUTE PRIVILEGED NETWORK ACCESSES*

The information system routes all networked, privileged accesses through a dedicated, managed interface for purposes of access control and auditing.

Supplemental Guidance: Related controls: AC-2, AC-3, AU-2, SI-4.

Deleted: Enhancement …upplemental …

(16) *BOUNDARY PROTECTION | PREVENT DISCOVERY OF COMPONENTS / DEVICES*

The information system prevents discovery of specific system components composing a managed interface.

Deleted: (or devices)

Deleted: Enhancement …upplemental …

Supplemental Guidance: This control enhancement protects network addresses of information system components that are part of managed interfaces from discovery through common tools and techniques used to identify devices on networks. Network addresses are not available for discovery (e.g., network address not published or entered in domain name systems), requiring prior knowledge for access. Another obfuscation technique is to periodically change network addresses.

(17) *BOUNDARY PROTECTION | AUTOMATED ENFORCEMENT OF PROTOCOL FORMATS*

The information system enforces adherence to protocol formats.

Deleted: The organization …

Deleted: Enhancement …upplemental …

Supplemental Guidance: Information system components that enforce protocol formats include, for example, deep packet inspection firewalls and XML gateways. Such system components verify adherence to protocol formats/specifications (e.g., IEEE) at the application layer and identify significant vulnerabilities that cannot be detected by devices operating at the network or transport layers. Related control: SC-4.

(18) *BOUNDARY PROTECTION | FAIL SECURE*

The information system fails securely in the event of an operational failure of a boundary protection device.

Deleted: Enhancement …upplemental …

Supplemental Guidance: Fail secure is a condition achieved by employing information system mechanisms to ensure that in the event of operational failures of boundary protection devices at managed interfaces (e.g., routers, firewalls, guards, and application gateways residing on protected subnetworks commonly referred to as demilitarized zones), information systems do not enter into unsecure states where intended security properties no longer hold. Failures of boundary protection devices cannot lead to, or cause information external to the devices to enter the devices, nor can failures permit unauthorized information releases. Related controls: CP-2, SC-24.

(19) *BOUNDARY PROTECTION | BLOCKS COMMUNICATION FROM NON-ORGANIZATIONALLY CONFIGURED HOSTS*

The information system blocks both inbound and outbound communications traffic between [*Assignment: organization-defined communication clients*] that are independently configured by end users and external service providers.

Supplemental Guidance: Communication clients independently configured by end users and external service providers include, for example, instant messaging clients. Traffic blocking does not apply to communication clients that are configured by organizations to perform authorized functions.

(20) *BOUNDARY PROTECTION | DYNAMIC ISOLATION / SEGREGATION*

The information system provides the capability to dynamically isolate/segregate [*Assignment: organization-defined information system components*] from other components of the system.

Supplemental Guidance: The capability to dynamically isolate or segregate certain internal components of organizational information systems is useful when it is necessary to partition or separate certain components of dubious origin from those components possessing greater trustworthiness. Component isolation reduces the attack surface of organizational information systems. Isolation of selected information system components is also a means of limiting the damage from successful cyber attacks when those attacks occur.

(21) *BOUNDARY PROTECTION | ISOLATION OF INFORMATION SYSTEM COMPONENTS*

The organization employs boundary protection mechanisms to separate [*Assignment: organization-defined information system components*] supporting [*Assignment: organization-defined missions and/or business functions*].

Supplemental Guidance: Organizations can isolate information system components performing different missions and/or business functions. Such isolation limits unauthorized information flows among system components and also provides the opportunity to deploy greater levels of protection for selected components. Separating system components with boundary protection mechanisms provides the capability for increased protection of individual components and to more effectively control information flows between those components. This type of enhanced protection limits the potential harm from cyber attacks and errors. The degree of separation provided varies depending upon the mechanisms chosen. Boundary protection mechanisms include, for example, routers, gateways, and firewalls separating system components into physically separate networks or subnetworks, cross-domain devices separating subnetworks, virtualization techniques, and encrypting information flows among system components using distinct encryption keys. Related controls: CA-9, SC-3.

(22) *BOUNDARY PROTECTION | SEPARATE SUBNETS FOR CONNECTING TO DIFFERENT SECURITY DOMAINS*

The information system implements separate network addresses (i.e., different subnets) to connect to systems in different security domains.

Supplemental Guidance: Decomposition of information systems into 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.

(23) *BOUNDARY PROTECTION | DISABLE SENDER FEEDBACK ON PROTOCOL VALIDATION FAILURE*

The information system disables feedback to senders on protocol format validation failure.

Supplemental Guidance: Disabling feedback to senders when there is a failure in protocol validation format prevents adversaries from obtaining information which would otherwise be unavailable.

References: FIPS Publication 199; NIST Special Publications 800-41, 800-77.

Priority and Baseline Allocation:

P1	**LOW** SC-7	**MOD** SC-7 (3) (4) (5) (7)	**HIGH** SC-7 (3) (4) (5) (7) (8) (18) (21)

Deleted: an

Deleted: state

Deleted: A failure

Deleted: a

Deleted: device

Deleted: boundary protection device

Deleted: device

Deleted: a failure

Deleted: release

Deleted: 1) (2) (

Deleted: 1) (2) (

Deleted: 6) (

SC-8 TRANSMISSION CONFIDENTIALITY AND INTEGRITY

Control: The information system protects the [*Selection (one or more): confidentiality; integrity*] of transmitted information.

Supplemental Guidance: This control applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification. Protecting the confidentiality and/or integrity of organizational information can be accomplished by physical means (e.g., by employing physical distribution systems) or by logical means (e.g., employing encryption techniques). Organizations relying on commercial providers offering transmission services as commodity services rather than as fully dedicated services (i.e., services which can be highly specialized to individual customer needs), may find it difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality/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 implement appropriate compensating security controls or explicitly accept the additional risk. Related controls: AC-17, PE-4.

Control Enhancements:

(1) *TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC OR ALTERNATE PHYSICAL PROTECTION*

The information system implements cryptographic mechanisms to [*Selection (one or more): prevent unauthorized disclosure of information; detect changes to information*] during transmission unless otherwise protected by [*Assignment: organization-defined alternative physical safeguards*].

Supplemental Guidance: Encrypting information for transmission protects information from unauthorized disclosure and modification. Cryptographic mechanisms implemented to protect information integrity include, for example, cryptographic hash functions which have common application in digital signatures, checksums, and message authentication codes. Alternative physical security safeguards include, for example, protected distribution systems. Related control: SC-13.

(2) *TRANSMISSION CONFIDENTIALITY AND INTEGRITY | PRE / POST TRANSMISSION HANDLING*

The information system maintains the [*Selection (one or more): confidentiality; integrity*] of information during preparation for transmission and during reception.

Supplemental Guidance: Information can be either unintentionally or maliciously disclosed or modified during preparation for transmission or during reception including, for example, during aggregation, at protocol transformation points, and during packing/unpacking. These unauthorized disclosures or modifications compromise the confidentiality or integrity of the information. Related control: AU-10.

(3) *TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC PROTECTION FOR MESSAGE EXTERNALS*

The information system implements cryptographic mechanisms to protect message externals unless otherwise protected by [*Assignment: organization-defined alternative physical safeguards*].

Supplemental Guidance: This control enhancement addresses protection against unauthorized disclosure of information. Message externals include, for example, message headers/routing information. This control enhancement prevents the exploitation of message externals and applies to both internal and external networks or links that may be visible to individuals who are not authorized users. Header/routing information is sometimes transmitted 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 and/or higher costs. Alternative physical safeguards include, for example, protected distribution systems. Related controls: SC-12, SC-13.

(4) *TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CONCEAL / RANDOMIZE COMMUNICATIONS*

Deleted: communications across

Deleted: . If

Deleted: organization is

Deleted: a

Deleted: service provider for

Deleted: a

Deleted: item

Deleted: a

Deleted: service, it

Deleted: be more

Deleted: integrity. When

Deleted: the organization either implements

Deleted: accepts

Deleted:

Deleted: organization employs

Deleted: recognize

Deleted: measures.

Deleted: Enhancement

Deleted: protection measures

Deleted:

Deleted: aggregation, packaging, and transformation in

Deleted: Enhancement

Deleted: intentionally and/

Deleted: at data aggregation or

Deleted: compromising

The information system implements cryptographic mechanisms to conceal or randomize communication patterns unless otherwise protected by [*Assignment: organization-defined alternative physical safeguards*].

Supplemental Guidance: This control enhancement addresses protection against unauthorized disclosure of information. Communication patterns include, for example, frequency, periods, amount, and predictability. Changes to communications patterns can reveal information having intelligence value especially when combined with other available information related to missions/business functions supported by organizational information systems. This control enhancement prevents the derivation of intelligence based on communications patterns and applies to both internal and external networks or links that may be visible to individuals who are not authorized users. Encrypting the links and transmitting in continuous, fixed/random patterns prevents the derivation of intelligence from the system communications patterns. Alternative physical safeguards include, for example, protected distribution systems. Related controls: SC-12, SC-13.

References: FIPS Publications 140-2, 197; NIST Special Publications 800-52, 800-77, 800-81, 800-113; CNSS Policy 15; NSTISSI No. 7003.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SC-8 (1)	**HIGH** SC-8 (1)

SC-9 TRANSMISSION CONFIDENTIALITY

[Withdrawn: Incorporated into SC-8].

SC-10 NETWORK DISCONNECT

Control: The information system terminates the network connection associated with a communications session at the end of the session or after [*Assignment: organization-defined time period*] of inactivity.

Supplemental Guidance: This control applies to both internal and external networks. Terminating network connections associated with communications sessions include, for example, de-allocating associated TCP/IP address/port pairs at the operating system level, or de-allocating networking assignments at the application level if multiple application sessions are using a single, operating system-level network connection. Time periods of inactivity may be established by organizations and include, for example, time periods by type of network access or for specific network accesses.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** SC-10	**HIGH** SC-10

SC-11 TRUSTED PATH

Control: The information system establishes a trusted communications path between the user and the following security functions of the system: [*Assignment: organization-defined security functions to include at a minimum, information system authentication and re-authentication*].

Deleted: Control: The information system protects the confidentiality of transmitted information.¶
Supplemental Guidance: This control applies to communications across internal and external networks. If the organization is relying on a commercial service provider for transmission services as a commodity item rather than a fully dedicated service, it may be more difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality. When it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. Related controls: AC-17, PE-4.¶
<#>The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures.¶
Enhancement Supplemental Guidance: Alternative physical protection measures include, for example, protected distribution systems. Related control: SC-13.¶
<#>The information system maintains the confidentiality of information during aggregation, packaging, and transformation in preparation for transmission.¶
Enhancement Supplemental Guidance: Information can be intentionally and/or maliciously disclosed at data aggregation or protocol transformation points, compromising the confidentiality of the information.

Deleted: References: FIPS Publications 140-2, 197; NIST Special Publications 800-52, 800-77, 800-113; CNSS Policy 15; NSTISSI No. 7003¶
P1 ...

Deleted:

Deleted: -

Deleted:

Deleted: The time period

Deleted: , as the organization deems necessary,

Deleted: a set of

Deleted: *reauthentication*

Supplemental Guidance: Trusted paths are mechanisms by which users (through input devices) can communicate directly with security functions of information systems with the requisite assurance to support information security policies. The mechanisms can be activated only by users or the security functions of organizational information systems. User responses via trusted paths are protected from modifications by or disclosure to untrusted applications. Organizations employ trusted paths for high-assurance connections between security functions of information systems and users (e.g., during system logons). Enforcement of trusted communications paths is typically provided via an implementation that meets the reference monitor concept. Related controls: AC-16, AC-25.

Deleted: A trusted path is employed for high-confidence connections between the security functions of the information system and the user (e.g., for login).

Control Enhancements:

Deleted: None

(1) *TRUSTED PATH | LOGICAL ISOLATION*

The information system provides a trusted communications path that is logically isolated and distinguishable from other paths.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

Control: The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [*Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction*].

Deleted: .

Supplemental Guidance: Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. Organizations define key management requirements in accordance with applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance, 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 information systems and certificates related to the internal operations of systems. Related controls: SC-13, SC-17.

Deleted: In addition to being required for the effective operation of a cryptographic mechanism, effective cryptographic

Deleted: provides protections

Deleted: maintain the availability of the

Deleted: in the event of the loss of cryptographic keys by users

Control Enhancements:

(1) *CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | AVAILABILITY*

The organization maintains availability of information in the event of the loss of cryptographic keys by users.

Supplemental Guidance: Escrowing of encryption keys is a common practice for ensuring availability in the event of loss of keys (e.g., due to forgotten passphrase).

(2) *CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | SYMMETRIC KEYS*

The organization produces, controls, and distributes symmetric cryptographic keys using [*Selection: NIST FIPS-compliant; NSA-approved*] key management technology and processes.

Deleted: *-approved,*

Deleted: The organization produces, controls, and distributes symmetric and asymmetric keys using NSA-approved technology and processes.

(3) *CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | ASYMMETRIC KEYS*

The organization produces, controls, and distributes asymmetric cryptographic keys using *[Selection: NSA-approved key management technology and processes; approved PKI Class 3 certificates or prepositioned keying material; approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user's private key].*

Deleted: .

Deleted: The organization produces, controls, and distributes asymmetric cryptographic keys using approved PKI Class 3 certificates or prepositioned keying material.¶

(4) *CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | PKI CERTIFICATES*

[Withdrawn: Incorporated into SC-12].

(5) *CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | PKI CERTIFICATES / HARDWARE TOKENS*

[Withdrawn: Incorporated into SC-12].

Deleted: The organization produces, controls, and distributes asymmetric cryptographic keys using approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user's private key.¶

References: NIST Special Publications 800-56, 800-57.

Priority and Baseline Allocation:

P1	**LOW** SC-12	**MOD** SC-12	**HIGH** SC-12 (1)

SC-13 CRYPTOGRAPHIC PROTECTION

Control: The information system implements [*Assignment: organization-defined* *cryptographic uses and type of cryptography required for each use*] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

Supplemental Guidance: Cryptography can be employed to support a variety of security solutions including, for example, the protection of classified and Controlled Unclassified Information, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information 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 based on the selection of other security controls, organizations define each type of cryptographic use and the type of cryptography required (e.g., protection of classified information: NSA-approved cryptography; provision of digital signatures: FIPS-validated cryptography). Related controls: AC-2, AC-3, AC-7, AC-17, AC-18, AU-9, AU-10, CM-11, CP-9, IA-3, IA-7, MA-4, MP-2, MP-4, MP-5, SA-4, SC-8, SC-12, SC-28, SI-7.

Control Enhancements: None.

(1) *CRYPTOGRAPHIC PROTECTION | FIPS-VALIDATED CRYPTOGRAPHY*
[Withdrawn: Incorporated into SC-13].

(2) *CRYPTOGRAPHIC PROTECTION | NSA-APPROVED CRYPTOGRAPHY*
[Withdrawn: Incorporated into SC-13].

(3) *CRYPTOGRAPHIC PROTECTION | INDIVIDUALS WITHOUT FORMAL ACCESS APPROVALS*
[Withdrawn: Incorporated into SC-13].

(4) *CRYPTOGRAPHIC PROTECTION | DIGITAL SIGNATURES*
[Withdrawn: Incorporated into SC-13].

References: FIPS Publication 140-2; Web: csrc.nist.gov/cryptval, www.cnss.gov.

Priority and Baseline Allocation:

P1	**LOW** SC-13	**MOD** SC-13	**HIGH** SC-13

SC-14 PUBLIC ACCESS PROTECTIONS

[Withdrawn: Capability provided by AC-2, AC-3, AC-5, AC-6, SI-3, SI-4, SI-5, SI-7, SI-10].

SC-15 COLLABORATIVE COMPUTING DEVICES

Control: The information system:

Deleted: USE OF CRYPTOGRAPHY

Deleted: required

Deleted: protections using cryptographic modules that comply

Deleted: , and guidance

Deleted: None.

Deleted: <#>The organization employs, at a minimum, FIPS-validated cryptography to protect unclassified information.¶
<#>The organization employs NSA-approved cryptography to protect classified information.¶
<#>The organization employs, at a minimum, FIPS-validated cryptography to protect information when such information must be separated from individuals who have the necessary clearances yet lack the necessary access approvals.¶
<#>The organization employs [*Selection: FIPS-validated; NSA-approved*] cryptography to implement digital signatures.¶

Deleted: Control: The information system protects the integrity and availability of publicly available information and applications.¶
Supplemental Guidance: The purpose of this control is to ensure that organizations explicitly address the protection needs for public information and applications with such protection likely being implemented as part of other security controls.

Moved up [8]: Control Enhancements: None.¶
References: None.¶
Priority and Baseline Allocation:¶

Deleted: P1 ...

a. Prohibits remote activation of collaborative computing devices with the following exceptions: [*Assignment: organization-defined exceptions where remote activation is to be allowed*]; and

b. Provides an explicit indication of use to users physically present at the devices.

Supplemental Guidance: Collaborative computing devices include, for example, networked white boards, cameras, and microphones. Explicit indication of use includes, for example, signals to users when collaborative computing devices are activated. Related control: AC-21.

Deleted:

Control Enhancements:

(1) *COLLABORATIVE COMPUTING DEVICES | PHYSICAL DISCONNECT*

The information system provides physical disconnect of collaborative computing devices in a manner that supports ease of use.

Supplemental Guidance: Failing to physically disconnect from collaborative computing devices can result in subsequent compromises of organizational information. Providing easy methods to physically disconnect from such devices after a collaborative computing session helps to ensure that participants actually carry out the disconnect activity without having to go through complex and tedious procedures.

(2) *COLLABORATIVE COMPUTING DEVICES | BLOCKING INBOUND / OUTBOUND COMMUNICATIONS TRAFFIC*

[Withdrawn: Incorporated into SC-7].

(3) *COLLABORATIVE COMPUTING DEVICES | DISABLING / REMOVAL IN SECURE WORK AREAS*

The organization disables or removes collaborative computing devices from [*Assignment: organization-defined information systems or information system components*] in [*Assignment: organization-defined secure work areas*].

Deleted: <#>The information system or supporting environment blocks both inbound and outbound traffic between instant messaging clients that are independently configured by end users and external service providers. ¶
Enhancement Supplemental Guidance: Blocking restrictions do not include instant messaging services that are configured by an organization to perform an authorized function.¶

Supplemental Guidance: Failing to disable or remove collaborative computing devices from information systems or information system components can result in subsequent compromises of organizational information including, for example, eavesdropping on conversations.

(4) *COLLABORATIVE COMPUTING DEVICES | EXPLICITLY INDICATE CURRENT PARTICIPANTS*

The information system provides an explicit indication of current participants in [*Assignment: organization-defined online meetings and teleconferences*].

Supplemental Guidance: This control enhancement helps to prevent unauthorized individuals from participating in collaborative computing sessions without the explicit knowledge of other participants.

References: None.

Priority and Baseline Allocation:

P1	**LOW** SC-15	**MOD** SC-15	**HIGH** SC-15

SC-16 TRANSMISSION OF SECURITY ATTRIBUTES

Control: The information system associates [*Assignment: organization-defined security attributes*] with information exchanged between information systems and between system components.

Supplemental Guidance: Security attributes can be explicitly or implicitly associated with the information contained in organizational information systems or system components. Related controls: AC-3, AC-4, AC-16.

Deleted: may

Deleted: within the

Deleted: .

Deleted: control

Control Enhancements:

(1) *TRANSMISSION OF SECURITY ATTRIBUTES | INTEGRITY VALIDATION*

The information system validates the integrity of transmitted security attributes.

Deleted: exchanged between systems

Supplemental Guidance: This control enhancement ensures that the verification of the integrity of transmitted information includes security attributes. Related controls: AU-10, SC-8.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES

Control: The organization issues public key certificates under an *[Assignment: organization-defined* certificate policy*]* or obtains public key certificates from an approved service provider.

Supplemental Guidance: For all certificates, organizations manage information system trust stores to ensure only approved trust anchors are in the trust stores. This control addresses both certificates with visibility external to organizational information systems and certificates related to the internal operations of systems, for example, application-specific time services. Related control: SC-12.

Control Enhancements: None.

References: OMB Memorandum 05-24; NIST Special Publications 800-32, 800-63.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SC-17	**HIGH** SC-17

Deleted: appropriate

Deleted: under an appropriate certificate policy

Deleted: user

Deleted: each organization attains

Deleted: from an approved, shared service provider, as required by OMB policy. For federal agencies operating a legacy public key infrastructure cross-certified

Deleted: the Federal Bridge Certification Authority at medium assurance or higher, this Certification Authority will suffice. This control focuses on certificates with a

Deleted: the

Deleted: system

Deleted: does not include

Deleted: system

SC-18 MOBILE CODE

Control: The organization:

a. Defines acceptable and unacceptable mobile code and mobile code technologies;

b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and

c. Authorizes, monitors, and controls the use of mobile code within the information system.

Supplemental Guidance: Decisions regarding the employment of mobile code within organizational information 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 guidance apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations and devices (e.g., smart phones). Mobile code policy and procedures address preventing the development, acquisition, or introduction of unacceptable mobile code within organizational information systems. Related controls: AU-2, AU-12, CM-2, CM-6, SI-3.

Control Enhancements:

(1) *MOBILE CODE | IDENTIFY UNACCEPTABLE CODE / TAKE CORRECTIVE ACTIONS*

The information system identifies [*Assignment: organization-defined unacceptable mobile code*] and takes [*Assignment: organization-defined corrective actions*].

Supplemental Guidance: Corrective actions when unacceptable mobile code is detected include, for example, blocking, quarantine, or alerting administrators. Blocking includes, for example, preventing transmission of word processing files with embedded macros when such macros have been defined to be unacceptable mobile code.

(2) *MOBILE CODE | ACQUISITION / DEVELOPMENT / USE*

The organization ensures that the acquisition, development, and use of mobile code to be deployed in the information system meets [*Assignment: organization-defined mobile code requirements*].

(3) *MOBILE CODE | PREVENT DOWNLOADING / EXECUTION*

Deleted: system

Deleted:

Deleted: PDF,

Deleted:

Deleted: organizational

Deleted: . Policy

Deleted: related to mobile code,

Deleted: the

Deleted: system

Deleted: implements detection and inspection mechanisms to identify unauthorized

Deleted: , when necessary.

Deleted: Enhancement

Deleted: unauthorized

Deleted: administrator. Disallowed transfers include

Deleted: sending

Deleted: /or

Deleted: systems

The information system prevents the download and execution of *[Assignment: organization-defined unacceptable* mobile code*]*.

Deleted: prohibited

Deleted: .

(4) *MOBILE CODE | PREVENT AUTOMATIC EXECUTION*

The information system prevents the automatic execution of mobile code in [*Assignment: organization-defined software applications*] and enforces [*Assignment: organization-defined actions*] prior to executing the code.

Deleted: requires

Supplemental Guidance: Actions enforced before executing mobile code, include, for example, prompting users prior to opening electronic mail attachments. Preventing automatic execution of mobile code includes, for example, disabling auto execute features on information system components employing portable storage devices such as Compact Disks (CDs), Digital Video Disks (DVDs), and Universal Serial Bus (USB) devices.

Deleted: Enhancement

Deleted: required

(5) *MOBILE CODE | ALLOW EXECUTION ONLY IN CONFINED ENVIRONMENTS*

The organization allows execution of permitted mobile code only in confined virtual machine environments.

References: NIST Special Publication 800-28; DoD Instruction 8552.01.

Deleted: DOD

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** SC-18	**HIGH** SC-18

Deleted: P1

SC-19 VOICE OVER INTERNET PROTOCOL

Control: The organization:

a. Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and

b. Authorizes, monitors, and controls the use of VoIP within the information system.

Supplemental Guidance: Related controls: CM-6, SC-7, SC-15.

Deleted: None

Control Enhancements: None.

References: NIST Special Publication 800-58.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SC-19	**HIGH** SC-19

SC-20 SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)

Control: The information system:

Deleted: provides

a. Provides additional data origin and integrity artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and

Deleted: .

b. Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

Supplemental Guidance: This control enables external clients including, for example, remote Internet clients, to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service. Information 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

Deleted: A

Deleted: server is an example of an information system that provides name/address resolution service. Digital

Deleted: are examples of additional artifacts.

authoritative data. The means to indicate the security status of child zones includes, for example, the use of delegation signer resource records in the DNS. The DNS security controls reflect (and are referenced from) OMB Memorandum 08-23. Information systems that use technologies other than the DNS to map between host/service names and network addresses provide other means to assure the authenticity and integrity of response data. Related controls: AU-10, SC-8, SC-12, SC-13, SC-21, SC-22.

Control Enhancements:

(1) *SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) | CHILD SUBSPACES*

[Withdrawn: Incorporated into SC-20].

(2) *SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) | DATA ORIGIN / INTEGRITY*

The information system provides data origin and integrity protection artifacts for internal name/address resolution queries.

References: OMB Memorandum 08-23; NIST Special Publication 800-81.

Priority and Baseline Allocation:

P1	**LOW** SC-20	**MOD** SC-20	**HIGH** SC-20

SC-21 SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)

Control: The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

Supplemental Guidance: Each client of name resolution services either performs this validation on its own, or has authenticated channels to trusted validation providers. Information 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. Information systems that use technologies other than the DNS to map between host/service names and network addresses provide other means to enable clients to verify the authenticity and integrity of response data. Related controls: SC-20, SC-22.

Control Enhancements: None.

(1) *SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER) | DATA ORIGIN / INTEGRITY*

[Withdrawn: Incorporated into SC-21].

References: NIST Special Publication 800-81.

Priority and Baseline Allocation:

P1	**LOW** SC-21	**MOD** SC-21	**HIGH** SC-21

SC-22 ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE

Control: The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.

Supplemental Guidance: Information 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

Deleted: The DNS security controls are consistent with, and referenced from, OMB Memorandum 08-23

Deleted: <#>The information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces and (if the child supports secure resolution services) enable verification of a chain of trust among parent and child domains.¶
Enhancement Supplemental Guidance: An example means to indicate the security status of child subspaces is through the use of delegation signer (DS) resource records in the DNS.¶

Deleted: (1)

Deleted: (1)

Deleted: (1)

Deleted: when requested by client systems

Deleted: A

Deleted: server is an example of an information system that provides name/address resolution service for local clients. Authoritative DNS

Deleted: are examples

Deleted: authoritative sources.

Deleted: <#>The information system performs data origin authentication and data integrity verification on all resolution responses whether or not local clients explicitly request this service.¶
Enhancement Supplemental Guidance: Local clients include, for example, DNS stub resolvers.¶

Deleted: Not Selected

Deleted: Not Selected

Deleted: A domain

Deleted: system (DNS) server is an example of an information system that provides name/

Deleted: service.

Deleted: there are typically

Deleted: (DNS)

Deleted: .

Deleted: two

Deleted: are commonly located

Deleted: different network subnets and

Deleted: With regard to

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 particular roles (e.g., by address ranges, explicit lists). Related controls: SC-2, SC-20, SC-21, SC-24.

Control Enhancements: None.

References: NIST Special Publication 800-81.

Priority and Baseline Allocation:

P1	**LOW** SC-22	**MOD** SC-22	**HIGH** SC-22

SC-23 SESSION AUTHENTICITY

Control: The information system protects the authenticity of communications sessions.

Supplemental Guidance: This control addresses communications protection at the session, versus packet level (e.g., sessions in service-oriented architectures providing web-based services) and establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted. Authenticity protection includes, for example, protecting against man-in-the-middle attacks/session hijacking and the insertion of false information into sessions. Related controls: SC-8, SC-10, SC-11.

Control Enhancements:

(1) *SESSION AUTHENTICITY | INVALIDATE SESSION IDENTIFIERS AT LOGOUT*

The information system invalidates session identifiers upon user logout or other session termination.

Supplemental Guidance: This control enhancement curtails the ability of adversaries from capturing and continuing to employ previously valid session IDs.

(2) *SESSION AUTHENTICITY | USER-INITIATED LOGOUTS / MESSAGE DISPLAYS*

[Withdrawn: Incorporated into AC-12 (1)].

(3) *SESSION AUTHENTICITY | UNIQUE SESSION IDENTIFIERS WITH RANDOMIZATION*

The information system generates a unique session identifier for each session with [*Assignment: organization-defined randomness requirements*] and recognizes only session identifiers that are system-generated.

Supplemental Guidance: This control enhancement curtails the ability of adversaries from reusing previously valid session IDs. Employing the concept of randomness in the generation of unique session identifiers helps to protect against brute-force attacks to determine future session identifiers. Related control: SC-13.

(4) *SESSION AUTHENTICITY | UNIQUE SESSION IDENTIFIERS WITH RANDOMIZATION*

(5) [Withdrawn: Incorporated into SC-23 (3)].

(5) *SESSION AUTHENTICITY | ALLOWED CERTIFICATE AUTHORITIES*

The information system only allows the use of [*Assignment: organization-defined certificate authorities*] for verification of the establishment of protected sessions.

Supplemental Guidance: Reliance on certificate authorities (CAs) for the establishment of secure sessions includes, for example, the use of Secure Socket Layer (SSL) and/or Transport Layer Security (TLS) certificates. These certificates, after verification by the respective certificate authorities, facilitate the establishment of protected sessions between web clients and web servers. Related control: SC-13.

References: NIST Special Publications 800-52, 800-77, 800-95.

Priority and Baseline Allocation:

Deleted: an

Deleted: role,

Deleted: /

Deleted: the organization

Deleted:

Deleted: an

Deleted: role

Deleted: /

Deleted: the organization

Deleted: the

Deleted: The set of

Deleted: an

Deleted: server

Deleted: a

Deleted: role is specified by the organization

Deleted: Not Selected

Deleted: provides mechanisms to protect

Deleted: focuses on

Deleted: ,

Deleted: . The intent of this control is to establish

Deleted: each end

Deleted: a

Deleted: session

Deleted: the

Deleted: identity

Deleted: the

Deleted: party

Deleted: the

Deleted: being

Deleted: For

Deleted: this control addresses

Deleted: including

Deleted: or

Deleted: a session. This control is only implemented where deemed necessary by the organization (e.g., sessions in service-oriented architectures providing web-based services).

Deleted: <#>The information system provides a readily observable logout capability whenever authentication is used to gain access to web pages.¶

Deleted: Enhancement

Deleted: The information system generates unique session identifiers w ...

P1	**LOW** Not Selected	**MOD** SC-23	**HIGH** SC-23

SC-24 FAIL IN KNOWN STATE

Control: The information system fails to a [*Assignment: organization-defined known-state*] for [*Assignment: organization-defined types of failures*] preserving [*Assignment: organization-defined system state information*] in failure.

Supplemental Guidance: Failure in a known state addresses security concerns in accordance with the mission/business needs of organizations. Failure in a known secure state helps to prevent the loss of confidentiality, integrity, or availability of information in the event of failures of organizational information 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 information system state information facilitates system restart and return to the operational mode of organizations with less disruption of mission/business processes. Related controls: CP-2, CP-10, CP-12, SC-7, SC-22.

Deleted: can address safety or

Deleted: the organization.

Deleted: a

Deleted: a failure

Deleted: the

Deleted: or a component of the system.

Deleted:

Deleted: the organization

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** Not Selected	**HIGH** SC-24

SC-25 THIN NODES

Control: The organization employs [*Assignment: organization-defined information system e*] with minimal functionality and information storage.

Deleted: employs processing

Deleted: that have

Supplemental Guidance: The deployment of information system components with reduced/minimal functionality (e.g., diskless nodes and thin client technologies) reduces the need to secure every user endpoint, and may reduce the exposure of information, information systems, and services to cyber attacks. Related control: SC-30.

Deleted: a successful attack.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-26 HONEYPOTS

Control: The information system includes components specifically designed to be the target of malicious attacks for the purpose of detecting, deflecting, and analyzing such attacks.

Supplemental Guidance: A honeypot is set up as a decoy to attract adversaries and to deflect their attacks away from the operational systems supporting organizational missions/business function. Depending upon the specific usage of the honeypot, consultation with the Office of the General Counsel before deployment may be needed. Related controls: SC-30, SC-44, SI-3, SI-4.

Deleted: ¶

Deleted: None.

Control Enhancements: None.

(1) *HONEYPOTS | DETECTION OF MALICIOUS CODE*
[Withdrawn: Incorporated into SC-35].

Deleted: The information system includes components that proactively seek to identify web-based malicious code.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

Deleted: Enhancement Supplemental Guidance: Devices that actively seek out web-based malicious code by posing as clients are referred to as client honeypots or honey clients.¶

SC-27 PLATFORM-INDEPENDENT APPLICATIONS

Control: The information system includes: [*Assignment: organization-defined platform-independent applications*].

Supplemental Guidance: Platforms are combinations of hardware and software used to run software applications. Platforms include: (i) operating systems; (ii) the underlying computer architectures, or (iii) both. Platform-independent applications are applications that run on multiple platforms. Such applications promote portability and reconstitution on different platforms, increasing the availability of critical functions within organizations while information systems with specific operating systems are under attack. Related control: SC-29.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

Deleted: OPERATING SYSTEM

Deleted: *operating system*

Deleted: Operating system

Deleted: can

Deleted: operating systems.

Deleted: platform architectures,

Deleted: for

Deleted: functionality

Deleted: an organization

Deleted: a given

Deleted: system

SC-28 PROTECTION OF INFORMATION AT REST

Control: The information system protects the [*Selection (one or more): confidentiality; integrity*] of [*Assignment: organization-defined* information at rest].

Supplemental Guidance: This control addresses the confidentiality and integrity of information at rest and covers user information and system information. Information at rest refers to the state of information when it is located on storage devices as specific components of information systems. System-related information requiring protection includes, for example, configurations or rule sets for firewalls, gateways, intrusion detection/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. Organizations may also employ other security controls including, for example, secure off-line storage in lieu of online storage when adequate protection of information at rest cannot otherwise be achieved and/or continuous monitoring to identify malicious code at rest. Related controls: AC-3, AC-6, CA-7, CM-3, CM-5, CM-6, PE-3, SC-8, SC-13, SI-3, SI-7.

Control Enhancements:

(1) *PROTECTION OF INFORMATION AT REST | CRYPTOGRAPHIC PROTECTION*

The information system implements cryptographic mechanisms to prevent unauthorized disclosure and modification of *[Assignment: organization-defined information]* on *[Assignment: organization-defined information system components]*.

Supplemental Guidance: Selection of cryptographic mechanisms is based on the need to protect the confidentiality and integrity of organizational information. The strength of mechanism is commensurate with the security category and/or classification of the information. This control enhancement applies to significant concentrations of digital media in organizational areas designated for media storage and also to limited quantities of media generally associated with information system components in operational environments (e.g., portable storage devices, mobile devices). Organizations have the flexibility to either encrypt all information on storage

Deleted: and

Deleted: .

Deleted: is intended to address

Deleted: in nonmobile devices

Deleted:

Deleted: a secondary

Deleted: device (e.g., disk drive, tape drive) within an organizational information system. Configurations and/

Deleted: and

Deleted: are examples of system information likely requiring protection.

Deleted: choose to

Deleted: as appropriate

Deleted: organization employs

Deleted: information at rest unless otherwise protected by alternative physical measures

devices (i.e., full disk encryption) or encrypt specific data structures (e.g., files, records, or fields). Organizations employing cryptographic mechanisms to protect information at rest also consider cryptographic key management solutions. Related controls: AC-19, SC-12.

(2) *PROTECTION OF INFORMATION AT REST | OFF-LINE STORAGE*

The organization removes from online storage and stores off-line in a secure location [*Assignment: organization-defined information*].

Supplemental Guidance: Removing organizational information from online information 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.

References: NIST Special Publications 800-56, 800-57, 800-111.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SC-28	**HIGH** SC-28

SC-29 HETEROGENEITY

Control: The organization employs a diverse set of information technologies for [*Assignment: organization-defined information system components*] in the implementation of the information system.

Supplemental Guidance: Increasing the diversity of information technologies within organizational information systems reduces the impact of potential exploitations of specific technologies and also defends 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 information system component will be equally effective against other system components, thus further increasing the adversary work factor to successfully complete planned cyber attacks. An increase in diversity may add complexity and management overhead which could ultimately lead to mistakes and unauthorized configurations. Related controls: SA-12, SA-14, SC-27.

Control Enhancements:

(1) *HETEROGENEITY | VIRTUALIZATION TECHNIQUES*

The organization employs virtualization techniques to support the deployment of a diversity of operating systems and applications that are changed [*Assignment: organization-defined frequency*].

Supplemental Guidance: While frequent changes to operating systems and applications pose configuration management challenges, the changes can result in an increased work factor for adversaries in order to carry out successful cyber attacks. Changing virtual operating systems or applications, as opposed to changing actual operating systems/applications, provide virtual changes that impede attacker success while reducing configuration management efforts. In addition, virtualization techniques can assist organizations in isolating untrustworthy software and/or software of dubious provenance into confined execution environments.

References: None.

Priority and Baseline Allocation:

Deleted: the

Deleted: system

Deleted: the exploitation of a specific technology. Organizations that select this control should consider that an

Deleted: , both of

Deleted: have the potential to

Deleted: misconfigurations which could increase overall risk

Deleted: None.

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-30 CONCEALMENT AND MISDIRECTION

Control: The organization employs [*Assignment: organization-defined concealment and misdirection techniques*] for [*Assignment: organization-defined information systems*] at [*Assignment: organization-defined time periods*] to confuse and mislead adversaries.

Supplemental Guidance: Concealment and misdirection techniques can significantly reduce the targeting capability of adversaries (i.e., window of opportunity and available attack surface) to initiate and complete cyber attacks. For example, virtualization techniques provide organizations with the ability to disguise information systems, potentially reducing the likelihood of successful attacks without the cost of having multiple platforms. Increased use of concealment/misdirection techniques 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/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/misdirection techniques, it is anticipated that such techniques would be used by organizations on a very limited basis. Related controls: SC-26, SC-29, SI-14.

Control Enhancements:

(1) *CONCEALMENT AND MISDIRECTION | VIRTUALIZATION TECHNIQUES*
[Withdrawn: Incorporated into SC-29 (1)].

(2) *CONCEALMENT AND MISDIRECTION | RANDOMNESS*
The organization employs [*Assignment: organization-defined techniques*] to introduce randomness into organizational operations and assets.

Supplemental Guidance: Randomness introduces increased levels of uncertainty for adversaries regarding the actions organizations take in defending against cyber attacks. Such actions may impede the ability of adversaries to correctly target information resources of organizations supporting critical missions/business functions. Uncertainty may also cause adversaries to hesitate before initiating or continuing attacks. Misdirection techniques involving randomness include, for example, performing certain routine actions at different times of day, employing different information technologies (e.g., browsers, search engines), using different suppliers, and rotating roles and responsibilities of organizational personnel.

(3) *CONCEALMENT AND MISDIRECTION | CHANGE PROCESSING / STORAGE LOCATIONS*
The organization changes the location of [*Assignment: organization-defined processing and/or storage*] [Selection: [*Assignment: organization-defined time frequency*]; *at random time intervals*]].

Supplemental Guidance: Adversaries target critical organizational missions/business functions and the information resources 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 information systems targeted by adversaries, make such systems more susceptible to cyber attacks with less adversary cost and effort to be successful. Changing organizational processing and storage locations (sometimes referred to as moving target defense) addresses the advanced persistent threat (APT) using techniques such as virtualization, distributed processing, and replication. This enables organizations to relocate the information resources (i.e., processing and/or storage) supporting critical missions and business functions. Changing locations of processing activities and/or storage sites introduces uncertainty into the targeting activities by adversaries. This uncertainty increases the work factor of adversaries making compromises or breaches to organizational information systems much more difficult and time-consuming, and increases the chances that adversaries may inadvertently disclose aspects of tradecraft while attempting to locate critical organizational resources.

(4) *CONCEALMENT AND MISDIRECTION | MISLEADING INFORMATION*

Deleted: VIRTUALIZATION TECHNIQUES

Deleted: The organization employs virtualization techniques to support the deployment of a diversity of operating systems and applications that are changed

Deleted: <#>Enhancement Supplemental Guidance: While frequent changes to operating systems and applications pose configuration management challenges, the changes result in an increased work factor for adversaries in order to carry out successful attacks. Changing the apparent operating system or application, as opposed to the actual operating system or application, results in virtual changes that still impede attacker success while helping to reduce the configuration management effort.¶

Deleted: randomness in the implementation of the virtualization techniques

The organization employs realistic, but misleading information in [*Assignment: organization-defined information system components*] with regard to its security state or posture.

Supplemental Guidance: This control enhancement misleads potential adversaries regarding the nature and extent of security safeguards deployed by organizations. As a result, adversaries may employ incorrect (and as a result ineffective) attack techniques. One way of misleading adversaries is for organizations to place misleading information regarding the specific security controls deployed in external information systems that are known to be accessed or targeted by adversaries. Another technique is the use of deception nets (e.g., honeynets, virtualized environments) that mimic actual aspects of organizational information systems but use, for example, out-of-date software configurations.

(5) *CONCEALMENT AND MISDIRECTION | CONCEALMENT OF SYSTEM COMPONENTS*

The organization employs [*Assignment: organization-defined techniques*] to hide or conceal [*Assignment: organization-defined information system components*].

Supplemental Guidance: By hiding, disguising, or otherwise concealing critical information system components, organizations may be able to decrease the probability that adversaries target and successfully compromise those assets. Potential means for organizations to hide and/or conceal information system components include, for example, configuration of routers or the use of honeynets or virtualization techniques.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-31 COVERT CHANNEL ANALYSIS

Control: The organization:

a. Performs a covert channel analysis to identify those aspects of communications within the information system that are potential avenues for covert [*Selection (one or more): storage; timing*] channels; and

b. Estimates the maximum bandwidth of those channels.

Supplemental Guidance: Developers are in the best position to identify potential areas within systems that might lead to covert channels. Covert channel analysis is a meaningful activity when there is the potential for unauthorized information flows across security domains, for example, in the case of information systems containing export-controlled information and having connections to external networks (i.e., networks not controlled by organizations). Covert channel analysis is also meaningful for multilevel secure (MLS) information systems, multiple security level (MSL) systems, and cross-domain systems. Related controls: AC-3, AC-4, PL-2.

Control Enhancements:

(1) *COVERT CHANNEL ANALYSIS | TEST COVERT CHANNELS FOR EXPLOITABILITY*

The organization tests a subset of the identified covert channels to determine which channels are exploitable.

(2) *COVERT CHANNEL ANALYSIS | MAXIMUM BANDWIDTH*

The organization reduces the maximum bandwidth for identified covert [*Selection (one or more); storage; timing*] channels to [*Assignment: organization-defined values*].

Supplemental Guidance: Information system developers are in the best position to reduce the maximum bandwidth for identified covert storage and timing channels.

(3) *COVERT CHANNEL ANALYSIS | MEASURE BANDWIDTH IN OPERATIONAL ENVIRONMENTS*

The organization measures the bandwidth of [*Assignment: organization-defined subset of identified covert channels*] in the operational environment of the information system.

Deleted: requires that information system developers/integrators perform

Deleted: communication

Deleted: and

Deleted: .

Deleted: Information system developers/integrators

Deleted: avenues

Deleted: the system

Deleted:

Deleted: the organization).

Deleted: in the case of

Deleted:

Deleted: vendor-

Deleted: channel avenues

Deleted: if they

Supplemental Guidance: This control enhancement addresses covert channel bandwidth in operational environments versus developmental environments. Measuring covert channel bandwidth in operational environments helps organizations to determine how much information can be covertly leaked before such leakage adversely affects organizational missions/business functions. Covert channel bandwidth may be significantly different when measured in those settings that are independent of the particular environments of operation (e.g., laboratories or development environments).

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-32 INFORMATION SYSTEM PARTITIONING

Control: The organization partitions the information system into [*Assignment: organization-defined information system components*] residing in separate physical domains or environments based on [*Assignment: organization-defined circumstances for physical separation of components*].

Supplemental Guidance: Information 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 more 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 information system components. Related controls: AC-4, SA-8, SC-2, SC-3, SC-7.

Control Enhancements: None.

References: FIPS Publication 199.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-33 TRANSMISSION PREPARATION INTEGRITY

[Withdrawn: Incorporated into SC-8].

SC-34 NON-MODIFIABLE EXECUTABLE PROGRAMS

Control: The information system at [*Assignment: organization-defined information system components*]:

a. Loads and executes the operating environment from hardware-enforced, read-only media; and

b. Loads and executes [*Assignment: organization-defined applications*] from hardware-enforced, read-only media.

Deleted: (

Deleted:) as deemed necessary.

Deleted: An organizational assessment of risk guides

Deleted: partitioning

Deleted: information

Deleted: into

Deleted: physical domains (or environments). The security

Deleted: also guides

Deleted: when system components can be associated with different system impact levels derived from the categorization.

Deleted:

Deleted: P1

Deleted: SC-32

Deleted: SC-32

Deleted: Control: The information system protects the integrity of information during the processes of data aggregation, packaging, and transformation in preparation for transmission.¶
Supplemental Guidance: Information can be subjected to unauthorized changes (e.g., malicious and/or unintentional modification) at information aggregation or protocol transformation points.¶
Control Enhancements: None.¶

Moved up [10]: References: None.¶
Priority and Baseline Allocation:¶
P0

Supplemental Guidance: The term *operating environment* is defined as 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)/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: (i) integrity can be adequately protected from the point of initial writing to the insertion of the memory into the information system; and (ii) there are reliable hardware protections against reprogramming the memory while installed in organizational information systems. Related controls: AC-3, SI-7.

Control Enhancements:

(1) *NON-MODIFIABLE EXECUTABLE PROGRAMS | NO WRITABLE STORAGE*

The organization employs [*Assignment: organization-defined information system components*] with no writeable storage that is persistent across component restart or power on/off.

Supplemental Guidance: This control enhancement: (i) eliminates the possibility of malicious code insertion via persistent, writeable storage within the designated information system components; and (ii) applies to both fixed and removable storage, with the latter being addressed directly or as specific restrictions imposed through access controls for mobile devices. Related controls: AC-19, MP-7.

(2) *NON-MODIFIABLE EXECUTABLE PROGRAMS | INTEGRITY PROTECTION / READ-ONLY MEDIA*

The organization protects the integrity of information prior to storage on read-only media and controls the media after such information has been recorded onto the media.

Supplemental Guidance: Security safeguards prevent the substitution of media into information systems or the reprogramming of programmable read-only media prior to installation into the systems. Security safeguards include, for example, a combination of prevention, detection, and response. Related controls: AC-5, CM-3, CM-5, CM-9, MP-2, MP-4, MP-5, SA-12, SC-28, SI-3.

(3) *NON-MODIFIABLE EXECUTABLE PROGRAMS | HARDWARE-BASED PROTECTION*

The organization:

(a) **Employs hardware-based, write-protect for [*Assignment: organization-defined information system firmware components*]; and**

(b) **Implements specific procedures for [*Assignment: organization-defined authorized individuals*] to manually disable hardware write-protect for firmware modifications and re-enable the write-protect prior to returning to operational mode.**

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-35 HONEYCLIENTS

Control: The information system includes components that proactively seek to identify malicious websites and/or web-based malicious code.

Supplemental Guidance: Honeyclients differ from honeypots in that the components actively probe the Internet in search of malicious code (e.g., worms) contained on external websites. As with honeypots, honeyclients require some supporting isolation measures (e.g., virtualization) to ensure that any malicious code discovered during the search and subsequently executed does not infect organizational information systems. Related controls: SC-26, SC-44, SI-3, SI-4.

References: None.

Deleted: In this control, the

Deleted: upon which

Deleted: are hosted

Deleted: a monitor, executive,

Deleted: system

Deleted: application

Deleted: the

Deleted: platform.

Deleted: /

Deleted: . Use

Deleted: the

Deleted: program

Deleted: Enhancement

Deleted: component

Deleted: requires no such

Deleted: be employed, a requirement that may be applied

Deleted: a

Deleted: restriction

Deleted: the

Deleted: ¶
Enhancement This control enhancement covers protecting the integrity of information to be placed onto read-only media

Deleted: controlling Protection measures may as deemed necessary by the organization

Deleted: and

Deleted: This enhancement may be satisfied by requirements imposed by other controls such as AC-3,

Deleted: and SI-7.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-36 DISTRIBUTED PROCESSING AND STORAGE

Control: The organization distributes [*Assignment: organization-defined processing and storage*] across multiple physical locations.

Supplemental Guidance: Distributing processing and storage across multiple physical locations provides some degree of redundancy or overlap for organizations, and therefore increases the work factor of adversaries to adversely impact organizational operations, assets, and individuals. This control does not assume a single primary processing or storage location, and thus allows for parallel processing and storage. Related controls: CP-6, CP-7.

Control Enhancements:

(1) *DISTRIBUTED PROCESSING AND STORAGE | POLLING TECHNIQUES*

The organization employs polling techniques to identify potential faults, errors, or compromises to [*Assignment: organization-defined distributed processing and storage components*].

Supplemental Guidance: Distributed processing and/or storage may be employed to reduce opportunities for adversaries to successfully compromise the confidentiality, integrity, or availability of information and information 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/or storage components. Related control: SI-4.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-37 OUT-OF-BAND CHANNELS

Control: The organization employs [*Assignment: organization-defined out-of-band channels*] for the physical delivery or electronic transmission of [*Assignment: organization-defined information, information system components, or devices*] to [*Assignment: organization-defined individuals or information systems*].

Supplemental Guidance: Out-of-band channels include, for example, local (nonnetwork) accesses to information 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/exposure as in-band channels, and hence the confidentiality, integrity, or availability compromises of in-band channels will not compromise 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/authenticators, configuration management changes for hardware, firmware, or software, cryptographic key management information, security updates, system/data backups, maintenance information, and malicious code protection updates. Related controls: AC-2, CM-3, CM-5, CM-7, IA-4, IA-5, MA-4, SC-12, SI-3, SI-4, SI-7.

Control Enhancements:

(1) *OUT-OF-BAND CHANNELS | ENSURE DELIVERY / TRANSMISSION*

The organization employs [*Assignment: organization-defined security safeguards*] to ensure that only [*Assignment: organization-defined individuals or information systems*] receive the [*Assignment: organization-defined information, information system components, or devices*].

Supplemental Guidance: Techniques and/or methods employed by organizations to ensure that only designated information systems or individuals receive particular information, system components, or devices include, for example, sending authenticators via courier service but requiring recipients to show some form of government-issued photographic identification as a condition of receipt.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-38 OPERATIONS SECURITY

Control: The organization employs [*Assignment: organization-defined operations security safeguards*] to protect key organizational information throughout the system development life cycle.

Supplemental Guidance: Operations security (OPSEC) is a systematic process by which potential adversaries can be denied information about the capabilities and intentions of organizations by identifying, controlling, and protecting generally unclassified information that specifically relates to the planning and execution of sensitive organizational activities. The OPSEC process involves five steps: (i) identification of critical information (e.g., the security categorization process); (ii) analysis of threats; (iii) analysis of vulnerabilities; (iv) assessment of risks; and (v) the application of appropriate countermeasures. OPSEC safeguards are applied to both organizational information systems and the environments in which those systems operate. OPSEC safeguards help to protect the confidentiality of key information including, for example, limiting the sharing of information with suppliers and potential suppliers of information system components, information technology products and services, and with other non-organizational elements and individuals. Information critical to mission/business success includes, for example, user identities, element uses, suppliers, supply chain processes, functional and security requirements, system design specifications, testing protocols, and security control implementation details. Related controls: RA-2, RA-5, SA-12.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-39 PROCESS ISOLATION

Control: The information system maintains a separate execution domain for each executing process.

Supplemental Guidance: Information systems can maintain separate execution domains for each executing process by assigning each process a separate address space. Each information 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 available in most commercial operating systems that employ multi-state processor technologies. Related controls: AC-3, AC-4, AC-6, SA-4, SA-5, SA-8, SC-2, SC-3.

Control Enhancements:

(1) *PROCESS ISOLATION | HARDWARE SEPARATION*

The information system implements underlying hardware separation mechanisms to facilitate process separation.

Supplemental Guidance: Hardware-based separation of information system processes is generally less susceptible to compromise than software-based separation, thus providing greater assurance that the separation will be enforced. Underlying hardware separation mechanisms include, for example, hardware memory management.

(2) *PROCESS ISOLATION | THREAD ISOLATION*

The information system maintains a separate execution domain for each thread in [*Assignment: organization-defined multi-threaded processing*].

References: None.

Priority and Baseline Allocation:

P1	**LOW** SC-39	**MOD** SC-39	**HIGH** SC-39

SC-40 WIRELESS LINK PROTECTION

Control: The information system protects external and internal [*Assignment: organization-defined wireless links*] from [*Assignment: organization-defined types of signal parameter attacks or references to sources for such attacks*].

Supplemental Guidance: This control applies to internal and external wireless communication links that may be visible to individuals who are not authorized information 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 to spoof users of organizational information systems. This control reduces the impact of attacks that are unique to wireless systems. If organizations rely on commercial service providers for transmission services as commodity items rather than as fully dedicated services, it may not be possible to implement this control. Related controls: AC-18, SC-5.

Control Enhancements:

(1) *WIRELESS LINK PROTECTION | ELECTROMAGNETIC INTERFERENCE*

The information system implements cryptographic mechanisms that achieve [*Assignment: organization-defined level of protection*] against the effects of intentional electromagnetic interference.

Supplemental Guidance: This control enhancement protects against intentional jamming that might deny or impair communications by ensuring that wireless spread spectrum waveforms used to provide anti-jam protection are not predictable by unauthorized individuals. The control enhancement may also coincidentally help to mitigate the effects of unintentional jamming due to interference from legitimate transmitters sharing the same spectrum. Mission requirements, projected threats, concept of operations, and applicable legislation, directives, regulations, policies, standards, and guidelines determine levels of wireless link availability and performance/cryptography needed. Related controls: SC-12, SC-13.

(2) *WIRELESS LINK PROTECTION | REDUCE DETECTION POTENTIAL*

The information system implements cryptographic mechanisms to reduce the detection potential of wireless links to [*Assignment: organization-defined level of reduction*].

Supplemental Guidance: This control enhancement is needed for covert communications and protecting wireless transmitters from being geo-located by their transmissions. The control enhancement ensures that spread spectrum waveforms used to achieve low probability of detection are not predictable by unauthorized individuals. Mission requirements, projected threats, concept of operations, and applicable legislation, directives, regulations, policies, standards, and guidelines determine the levels to which wireless links should be undetectable. Related controls: SC-12, SC-13.

(3) *WIRELESS LINK PROTECTION | IMITATIVE OR MANIPULATIVE COMMUNICATIONS DECEPTION*

The information system implements cryptographic mechanisms to identify and reject wireless transmissions that are deliberate attempts to achieve imitative or manipulative communications deception based on signal parameters.

Supplemental Guidance: This control enhancement ensures that the signal parameters of wireless transmissions are not predictable by unauthorized individuals. Such unpredictability reduces the probability of imitative or manipulative communications deception based upon signal parameters alone. Related controls: SC-12, SC-13.

(4) *WIRELESS LINK PROTECTION | SIGNAL PARAMETER IDENTIFICATION*

The information system implements cryptographic mechanisms to prevent the identification of [*Assignment: organization-defined wireless transmitters*] by using the transmitter signal parameters.

Supplemental Guidance: Radio fingerprinting techniques identify the unique signal parameters of transmitters to fingerprint such transmitters for purposes of tracking and mission/user identification. This control enhancement protects against the unique identification of wireless transmitters for purposes of intelligence exploitation by ensuring that anti-fingerprinting alterations to signal parameters are not predictable by unauthorized individuals. This control enhancement helps assure mission success when anonymity is required. Related controls: SC-12, SC-13.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-41 PORT AND I/O DEVICE ACCESS

Control: The organization physically disables or removes [*Assignment: organization-defined connection ports or input/output devices*] on [*Assignment: organization-defined information systems or information system components*].

Supplemental Guidance: Connection ports include, for example, Universal Serial Bus (USB) and Firewire (IEEE 1394). Input/output (I/O) devices include, for example, Compact Disk (CD) and Digital Video Disk (DVD) drives. Physically disabling or removing such connection ports and I/O devices helps prevent exfiltration of information from information systems and the introduction of malicious code into systems from those ports/devices.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-42 SENSOR CAPABILITY AND DATA

Control: The information system:

a. Prohibits the remote activation of environmental sensing capabilities with the following exceptions: [*Assignment: organization-defined exceptions where remote activation of sensors is allowed*]; and

b. Provides an explicit indication of sensor use to [*Assignment: organization-defined class of users*].

Supplemental Guidance: This control often applies to types of information 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.

Control Enhancements:

(1) *SENSOR CAPABILITY AND DATA | REPORTING TO AUTHORIZED INDIVIDUALS OR ROLES*

The organization ensures that the information system is configured so that data or information collected by the [*Assignment: organization-defined sensors*] is only reported to authorized individuals or roles.

Supplemental Guidance: In situations where sensors are activated by authorized individuals (e.g., end users), it is still possible that the data/information collected by the sensors will be sent to unauthorized entities.

(2) *SENSOR CAPABILITY AND DATA | AUTHORIZED USE*

The organization employs the following measures: [*Assignment: organization-defined measures*], so that data or information collected by [*Assignment: organization-defined sensors*] is only used for authorized purposes.

Supplemental Guidance: Information collected by sensors for a specific authorized purpose potentially 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 parties do not abuse their authority, or (in the case where sensor data/information is maintained by external parties) contractual restrictions on the use of the data/information.

(3) *SENSOR CAPABILITY AND DATA | PROHIBIT USE OF DEVICES*

The organization prohibits the use of devices possessing [*Assignment: organization-defined environmental sensing capabilities*] in [*Assignment: organization-defined facilities, areas, or systems*].

Supplemental Guidance: For example, organizations may prohibit individuals from bringing cell phones or digital cameras into certain facilities or specific controlled areas within facilities where classified information is stored or sensitive conversations are taking place.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-43 USAGE RESTRICTIONS

Control: The organization:

a. Establishes usage restrictions and implementation guidance for [*Assignment: organization-defined information system components*] based on the potential to cause damage to the information system if used maliciously; and

b. Authorizes, monitors, and controls the use of such components within the information system.

Supplemental Guidance: Information system components include hardware, software, or firmware components (e.g., Voice Over Internet Protocol, mobile code, digital copiers, printers, scanners, optical devices, wireless technologies, mobile devices). Related controls: CM-6, SC-7.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-44 DETONATION CHAMBERS

Control: The organization employs a detonation chamber capability within [*Assignment: organization-defined information system, system component, or location*].

Supplemental Guidance: Detonation chambers, also known as dynamic execution environments, allow organizations to open email attachments, execute untrusted or suspicious applications, and execute Universal Resource Locator (URL) requests in the safety of an isolated environment or virtualized sandbox. These protected and isolated execution environments provide a means of determining whether the associated attachments/applications contain malicious code. While related to the concept of deception nets, the control is not intended to maintain a long-term environment in which adversaries can operate and their actions can be observed. Rather, it is intended to quickly identify malicious code and reduce the likelihood that the code is propagated to user environments of operation (or prevent such propagation completely). Related controls: SC-7, SC-25, SC-26, SC-30.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

FAMILY: SYSTEM AND INFORMATION INTEGRITY

SI-1 SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

1. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and

b. Reviews and updates the current:

1. System and information integrity policy [*Assignment: organization-defined frequency*]; and

2. System and information integrity procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the SI family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

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

Priority and Baseline Allocation:

P1	**LOW** SI-1	**MOD** SI-1	**HIGH** SI-1

SI-2 FLAW REMEDIATION

Control: The organization:

a. Identifies, reports, and corrects information system flaws;

b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;

c. Installs security-relevant software and firmware updates within [*Assignment: organization-defined time period*] of the release of the updates; and

d. Incorporates flaw remediation into the organizational configuration management process.

Supplemental Guidance: Organizations identify information systems affected by announced software flaws including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security responsibilities. Security-relevant software updates include, for example, patches, service packs, hot fixes, and anti-virus signatures. Organizations also address flaws discovered during security assessments,

Deleted: **CLASS:** OPERATIONAL

Deleted: develops,

Deleted: , and reviews/updates

Deleted: *frequency*

Deleted: A formal, documented

Deleted: Formal, documented procedures

Deleted: .

Deleted: is intended to produce

Deleted: that are required

Deleted: system and information integrity

Deleted: The policy

Deleted: are consistent with

Deleted: policies,

Deleted: Existing organizational

Deleted: additional

Deleted:

Deleted: system and information integrity

Deleted: the organization. System and information integrity

Deleted: developed

Deleted: a

Deleted: system, when required.

Deleted: the development of the system and information integrity

Deleted: .

Deleted: on organizational information systems

Deleted: The organization identifies

Deleted: containing software

Deleted: recently

Deleted: (and

Deleted:)

Deleted: reports

Deleted: officials

Deleted: (e.g., senior information security officers, information system security managers, information systems security officers). The organization (including any contractor to the organization) promptly installs security-relevant software

Deleted: (e.g.,

Deleted: and

Deleted:). Flaws

continuous monitoring, incident response activities, and system error handling. Organizations take advantage of available resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases in remediating flaws discovered in organizational information systems. By incorporating flaw remediation into ongoing configuration management processes, required/anticipated remediation actions can be tracked and verified. Flaw remediation actions that can be tracked and verified include, for example, determining whether organizations follow US-CERT guidance and Information Assurance Vulnerability Alerts. Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of factors including, for example, the security category of the information system or the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw). Some types of flaw remediation may require more testing than other types. Organizations determine the degree and type of testing needed for the specific type of flaw remediation activity under consideration and also the types of changes that are to be configuration-managed. In some situations, organizations may determine that the testing of software and/or firmware updates is not necessary or practical, for example, when implementing simple anti-virus signature updates. Organizations may also consider in testing decisions, whether security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures. Related controls: CA-2, CA-7, CM-3, CM-5, CM-8, MA-2, IR-4, RA-5, SA-10, SA-11, SI-11.

Deleted: or information

Deleted: , are also addressed expeditiously.

Deleted: are encouraged to use

Deleted:

Deleted: requiring that

Deleted: be incorporated

Deleted: the organizational

Deleted: process, it is the intent of this control that

Deleted: are

Deleted: An example of expected flaw

Deleted: would

Deleted: so

Deleted: is

Deleted: the procedures contained in

Deleted: have been accomplished.

Control Enhancements:

(1) *FLAW REMEDIATION | CENTRAL MANAGEMENT*

The organization centrally manages the flaw remediation process.

Supplemental Guidance: Central management is the organization-wide management and implementation of flaw remediation processes. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed flaw remediation security controls.

(2) *FLAW REMEDIATION | AUTOMATED FLAW REMEDIATION STATUS*

The organization employs automated mechanisms [*Assignment: organization-defined frequency*] to determine the state of information system components with regard to flaw remediation.

Supplemental Guidance: Related controls: CM-6, SI-4.

Deleted: Enhancement Supplemental Guidance: Due to information system integrity and availability concerns, organizations give careful consideration to the methodology used to carry out automatic updates.¶

(3) *FLAW REMEDIATION | TIME TO REMEDIATE FLAWS / BENCHMARKS FOR CORRECTIVE ACTIONS*

The organization:

(a) Measures the time between flaw identification and flaw remediation; and

Deleted: , comparing with

(b) Establishes [*Assignment: organization-defined benchmarks*] for taking corrective actions.

Supplemental Guidance: This control enhancement requires organizations to determine the current time it takes on the average to correct information 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 type of flaw and/or severity of the potential vulnerability if the flaw can be exploited.

(4) *FLAW REMEDIATION | AUTOMATED PATCH MANAGEMENT TOOLS*

(5) [Withdrawn: Incorporated into SI-2].

(5) *FLAW REMEDIATION | AUTOMATIC SOFTWARE / FIRMWARE UPDATES*

The organization installs [*Assignment: organization-defined security-relevant software and firmware updates*] automatically to [*Assignment: organization-defined information system components*].

Deleted: The organization employs automated patch management tools to facilitate flaw remediation to [*Assignment: organization-defined information system components*].¶

Supplemental Guidance: Due to information system integrity and availability concerns, organizations give careful consideration to the methodology used to carry out automatic updates. Organizations must balance the need to ensure that the updates are installed as soon as possible with the need to maintain configuration management and with any mission or operational impacts that automatic updates might impose.

(6) *FLAW REMEDIATION | REMOVAL OF PREVIOUS VERSIONS OF SOFTWARE / FIRMWARE*

The organization removes [*Assignment: organization-defined software and firmware components*] after updated versions have been installed.

Supplemental Guidance: Previous versions of software and/or firmware components that are not removed from the information system after updates have been installed may be exploited by adversaries. Some information technology products may remove older versions of software and/or firmware automatically from the information system.

References: NIST Special Publications 800-40, 800-128..

Priority and Baseline Allocation:

P1	**LOW** SI-2	**MOD** SI-2 (2)	**HIGH** SI-2 (1) (2)

SI-3 MALICIOUS CODE PROTECTION

Control: The organization:

a. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;

b. Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures;

c. Configures malicious code protection mechanisms to:

1. Perform periodic scans of the information system [*Assignment: organization-defined frequency*] and real-time scans of files from external sources at [*Selection (one or more); endpoint; network entry/exit points*] as the files are downloaded, opened, or executed in accordance with organizational security policy; and

2. [*Selection (one or more): block malicious code; quarantine malicious code; send alert to administrator;* [*Assignment: organization-defined action*]] in response to malicious code detection; and

d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

Supplemental Guidance: Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, notebook computers, and mobile devices. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files, or hidden in files using steganography. Malicious code can be transported by different means including, for example, web accesses, electronic mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitation of information system vulnerabilities. Malicious code protection mechanisms include, for example, anti-virus signature definitions and reputation-based technologies. A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, organizations rely instead on other 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, and/or actions in response to detection of maliciousness when attempting to open or execute files. Related controls: CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7.

Deleted: Publication

Deleted: and at workstations, servers, or mobile computing devices on the network

Deleted: :

Deleted: <#>Transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; or¶
<#>Inserted through the exploitation of information system vulnerabilities;¶

Deleted: (including signature definitions)

Deleted: and

Deleted: .

Deleted:

Deleted:) or

Deleted: a

Deleted: file. Removable media includes

Deleted: USB devices, diskettes, or compact disks.

Deleted: attacks.

Deleted: strong

Deleted:

Deleted:

Deleted: and

Deleted:

Deleted: are not built to

Deleted:

Deleted: must

Deleted: risk mitigation measures to include

Deleted: trusted procurement processes,

Deleted: those

Control Enhancements:

(1) *MALICIOUS CODE PROTECTION | CENTRAL MANAGEMENT*

The organization centrally manages malicious code protection mechanisms.

Supplemental Guidance: Central management is the organization-wide management and implementation of malicious code protection mechanisms. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed flaw malicious code protection security controls. Related controls: AU-2, SI-8.

(2) *MALICIOUS CODE PROTECTION | AUTOMATIC UPDATES*

The information system automatically updates malicious code protection mechanisms.

Deleted: (including

Supplemental Guidance: Malicious code protection mechanisms include, for example, signature definitions. Due to information system integrity and availability concerns, organizations give careful consideration to the methodology used to carry out automatic updates. Related control: SI-8.

Deleted:).

(3) *MALICIOUS CODE PROTECTION | NON-PRIVILEGED USERS*

[Withdrawn: Incorporated into AC-6 (10)].

Deleted: The information system prevents non-privileged users from circumventing

Deleted: malicious code protection capabilities.

(4) *MALICIOUS CODE PROTECTION | UPDATES ONLY BY PRIVILEGED USERS*

The information system updates malicious code protection mechanisms only when directed by a privileged user.

Supplemental Guidance: This control enhancement may be appropriate for situations where for reasons of security or operational continuity, updates are only applied when selected/approved by designated organizational personnel. Related controls: AC-6, CM-5.

(5) *MALICIOUS CODE PROTECTION | PORTABLE STORAGE DEVICES*

[Withdrawn: Incorporated into MP-7].

Deleted: The organization does not allow users to introduce removable media into the information system.

(6) *MALICIOUS CODE PROTECTION | TESTING / VERIFICATION*

The organization:

(a) Tests malicious code protection mechanisms [*Assignment: organization-defined frequency*] by introducing a known benign, non-spreading test case into the information system; and

(b) Verifies that both detection of the test case and associated incident reporting occur.

Deleted: and subsequently verifying , as required.

Supplemental Guidance: Related controls: CA-2, CA-7, RA-5.

(7) *MALICIOUS CODE PROTECTION | NONSIGNATURE-BASED DETECTION*

The information system implements nonsignature-based malicious code detection mechanisms.

Supplemental Guidance: Nonsignature-based detection mechanisms include, for example, the use of heuristics to detect, analyze, and describe the characteristics or behavior of malicious code and to provide safeguards against malicious code for which signatures do not yet exist or for which existing signatures may not be effective. This includes polymorphic malicious code (i.e., code that changes signatures when it replicates). This control enhancement does not preclude the use of signature-based detection mechanisms.

(8) *MALICIOUS CODE PROTECTION | DETECT UNAUTHORIZED COMMANDS*

The information system detects [*Assignment: organization-defined unauthorized operating system commands*] through the kernel application programming interface at [*Assignment: organization-defined information system hardware components*] and [*Selection (one or more): issues a warning; audits the command execution; prevents the execution of the command*].

Supplemental Guidance: This control enhancement can also be applied to critical interfaces other than kernel-based interfaces, including for example, interfaces with virtual machines and privileged applications. Unauthorized operating system commands include, for example, commands for kernel functions from information system processes that are not trusted to initiate such commands, or commands for kernel functions that are suspicious even though commands of that type are reasonable for processes to initiate. Organizations can define the malicious commands to be detected by a combination of command types, command classes, or specific instances of commands. Organizations can define hardware components by specific component, component type, location in the network, or combination therein. Organizations may select different actions for different types/classes/specific instances of potentially malicious commands. Related control: AU-6.

(9) *MALICIOUS CODE PROTECTION | AUTHENTICATE REMOTE COMMANDS*

The information system implements [*Assignment: organization-defined security safeguards*] to authenticate [*Assignment: organization-defined remote commands*].

Supplemental Guidance: This control enhancement protects against unauthorized commands and replay of authorized commands. This capability is important for those remote information systems whose loss, malfunction, misdirection, or exploitation would have immediate and/or serious consequences (e.g., injury or death, property damage, loss of high-valued assets or sensitive information, or failure of important missions/business functions). Authentication safeguards for remote commands help to ensure that information systems accept and execute in the order intended, only authorized commands, and that unauthorized commands are rejected. Cryptographic mechanisms can be employed, for example, to authenticate remote commands. Related controls: SC-12, SC-13, SC-23.

(10) *MALICIOUS CODE PROTECTION | MALICIOUS CODE ANALYSIS*

The organization:

(a) Employs [*Assignment: organization-defined tools and techniques*] to analyze the characteristics and behavior of malicious code; and

(b) Incorporates the results from malicious code analysis into organizational incident response and flaw remediation processes.

Supplemental Guidance: The application of selected malicious code analysis tools and techniques provides organizations with a more in-depth understanding of adversary tradecraft (i.e., tactics, techniques, and procedures) and the functionality and purpose of specific instances of malicious code. Understanding the characteristics of malicious code facilitates more effective organizational responses to current and future threats. Organizations can conduct malicious code analyses by using reverse engineering techniques or by monitoring the behavior of executing code.

References: NIST Special Publication 800-83.

Priority and Baseline Allocation:

P1	**LOW** SI-3	**MOD** SI-3 (1) (2)	**HIGH** SI-3 (1) (2)

Deleted: (3)

Deleted: (3)

SI-4 INFORMATION SYSTEM MONITORING

Control: The organization:

a. Monitors the information system to detect:

Deleted: events on

1. Attacks and indicators of potential attacks in accordance with [*Assignment: organization-defined monitoring objectives*]; and

Deleted:] and detects information system attacks;

2. Unauthorized local, network, and remote connections;

b. Identifies unauthorized use of the information system through [*Assignment: organization-defined techniques and methods*];

Deleted: ;

c. Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization;

d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;

e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information;

f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and

g. Provides [*Assignment: organization-defined information system monitoring information*] to [*Assignment: organization-defined personnel or roles*] [*Selection (one or more): as needed; [Assignment: organization-defined frequency*]].

Supplemental Guidance: Information system monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the information system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the information system. Organizations can monitor information systems, for example, by observing audit activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions. The monitoring objectives may guide determination of the events. Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring software). Strategic locations for monitoring devices include, for example, selected perimeter locations and near server farms supporting critical applications, with such devices typically being employed at the managed interfaces associated with controls SC-7 and AC-17. Einstein network monitoring devices from the Department of Homeland Security can also be included as monitoring devices. The granularity of monitoring information collected is based on organizational monitoring objectives and the capability of information systems to support such objectives. Specific types of transactions of interest include, for example, Hyper Text Transfer Protocol (HTTP) traffic that bypasses HTTP proxies. Information system monitoring is an integral part of organizational continuous monitoring and incident response programs. Output from system monitoring serves as input to continuous monitoring and incident response programs. A network connection is any connection with a device that communicates through a network (e.g., local area network, Internet). A remote connection is any connection with a device communicating through an external network (e.g., the Internet). Local, network, and remote connections can be either wired or wireless. Related controls: AC-3, AC-4, AC-8, AC-17, AU-2, AU-6, AU-7, AU-9, AU-12, CA-7, IR-4, PE-3, RA-5, SC-7, SC-26, SC-35, SI-3, SI-7.

Control Enhancements:

(1) *INFORMATION SYSTEM MONITORING | SYSTEM-WIDE INTRUSION DETECTION SYSTEM*

The organization connects and configures individual intrusion detection tools into an information system-wide intrusion detection system.

(2) *INFORMATION SYSTEM MONITORING | AUTOMATED TOOLS FOR REAL-TIME ANALYSIS*

The organization employs automated tools to support near real-time analysis of events.

Supplemental Guidance: Automated tools include, for example, host-based, network-based, transport-based, or storage-based event monitoring tools or Security Information and Event Management (SIEM) technologies that provide real time analysis of alerts and/or notifications generated by organizational information systems.

(3) *INFORMATION SYSTEM MONITORING | AUTOMATED TOOL INTEGRATION*

The organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination.

(4) *INFORMATION SYSTEM MONITORING | INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC*

The information system monitors inbound and outbound communications traffic [*Assignment: organization-defined frequency*] for unusual or unauthorized activities or conditions.

Supplemental Guidance: Unusual/unauthorized activities or conditions related to information system inbound and outbound communications traffic include, for example, internal traffic that indicates the presence of malicious code within organizational information systems or

Deleted: and

Deleted: .

Deleted:

Deleted:

Deleted: system (e.g., within internal organizational networks and system components).

Deleted:

Deleted: at

Deleted: The

Deleted: device

Deleted: is an example of a system

Deleted: device

Deleted: the

Deleted: determined by the organization

Deleted: its

Deleted: the

Deleted: system

Deleted: activities. An example of a specific type

Deleted: transaction

Deleted: to the organization with regard to monitoring is

Deleted: organizational

Deleted: , when use of such proxies is required.

Deleted: interconnects

Deleted: a systemwide

Deleted: using common protocols

Deleted: Enhancement

Deleted: an

Deleted: system

propagating among system components, the unauthorized exporting of information, or signaling to external information systems. Evidence of malicious code is used to identify potentially compromised information systems or information system components.

(5) *INFORMATION SYSTEM MONITORING | SYSTEM-GENERATED ALERTS*

The information system alerts [*Assignment: organization-defined personnel or roles*] when the following indications of compromise or potential compromise occur: [*Assignment: organization-defined compromise indicators*].

Supplemental Guidance: Alerts may be generated from a variety of sources, including, for example, audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers. Alerts can be transmitted, for example, telephonically, by electronic mail messages, or by text messaging. Organizational personnel on the notification list can include, for example, system administrators, mission/business owners, system owners, or information system security officers. Related controls: AU-5, PE-6.

(6) *INFORMATION SYSTEM MONITORING | RESTRICT NON-PRIVILEGED USERS*

[Withdrawn: Incorporated into AC-6 (10)].

(7) *INFORMATION SYSTEM MONITORING | AUTOMATED RESPONSE TO SUSPICIOUS EVENTS*

The information system notifies [*Assignment: organization-defined incident response personnel (identified by name and/or by role)*] of detected suspicious events and takes [*Assignment: organization-defined least-disruptive actions to terminate suspicious events*].

Supplemental Guidance: Least-disruptive actions may include, for example, initiating requests for human responses.

(8) *INFORMATION SYSTEM MONITORING | PROTECTION OF MONITORING INFORMATION*

[Withdrawn: Incorporated into SI-4].

(9) *INFORMATION SYSTEM MONITORING | TESTING OF MONITORING TOOLS*

The organization tests intrusion-monitoring tools [*Assignment: organization-defined frequency*].

Supplemental Guidance: Testing intrusion-monitoring tools is necessary to ensure that the tools are operating correctly and continue to meet the monitoring objectives of organizations. The frequency of testing depends on the types of tools used by organizations and methods of deployment. Related control: CP-9.

(10) *INFORMATION SYSTEM MONITORING | VISIBILITY OF ENCRYPTED COMMUNICATIONS*

The organization makes provisions so that [*Assignment: organization-defined encrypted communications traffic*] is visible to [*Assignment: organization-defined information system monitoring tools*].

Supplemental Guidance: Organizations balance the potentially conflicting needs for encrypting communications traffic and for having insight into such traffic from a monitoring perspective. For some organizations, the need to ensure the confidentiality of communications traffic is paramount; for others, 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.

(11) *INFORMATION SYSTEM MONITORING | ANALYZE COMMUNICATIONS TRAFFIC ANOMALIES*

The organization analyzes outbound communications traffic at the external boundary of the information system and selected [*Assignment: organization-defined interior points within the system (e.g., subnetworks, subsystems)*] to discover anomalies.

Supplemental Guidance: Anomalies within organizational information 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.

(12) *INFORMATION SYSTEM MONITORING | AUTOMATED ALERTS*

The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: [*Assignment: organization-defined activities that trigger alerts*].

Deleted: export

Deleted: an

Deleted: system.

Deleted: provides near real-time alerts

Deleted: ***list of***

Deleted: Enhancement

Deleted: , depending on the organization-defined list of indicators,

Deleted: input

Deleted: The information system prevents non-privileged users from circumventing intrusion detection and prevention capabilities.

Deleted: ***list of***

Deleted: ***list of***

Deleted: Enhancement

Deleted: The least

Deleted: a request

Deleted: response

Deleted: The organization protects information obtained from intrusion- ...

Deleted: /exercises

Deleted: Enhancement

Deleted: /exercises is dependent upon

Deleted: type

Deleted: method

Deleted: of the intrusion-monitoring tools

Deleted: .

Deleted: Enhancement

Deleted: The enhancement recognizes the ...

Deleted: versus the need to have

Deleted: that

Deleted:

Deleted: the

Deleted: concerns are

Deleted: (i.e., system perimeter)

Deleted: , as deemed necessary, at

Deleted: subnets

Deleted:)

Deleted: Enhancement

Deleted: the

Deleted: system

Deleted:

Deleted: ***list of inappropriate or unusual***

Supplemental Guidance: This control enhancement focuses on the security alerts generated by organizations and transmitted using automated means. In contrast to the alerts generated by information systems in SI-4 (5), which tend to focus on information sources internal to the systems (e.g., audit records), the sources of information for this enhancement can include other entities as well (e.g., suspicious activity reports, reports on potential insider threats). Related controls: AC-18, IA-3.

(13) *INFORMATION SYSTEM MONITORING | ANALYZE TRAFFIC / EVENT PATTERNS*

The organization:

(a) Analyzes communications traffic/event patterns for the information system;

(b) Develops profiles representing common traffic patterns and/or events; and

(c) Uses the traffic/event profiles in tuning system-monitoring devices to reduce the number of false positives and the number of false negatives.

Deleted: to [*Assignment: organization-defined measure of false positives*]

Deleted: to [*Assignment: organization-defined measure of false negatives*].

(14) *INFORMATION SYSTEM MONITORING | WIRELESS INTRUSION DETECTION*

The organization employs a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system.

Supplemental Guidance: Wireless signals may radiate beyond the confines of 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 information systems, but also include areas outside of facilities as needed, to verify that unauthorized wireless access points are not connected to the systems. Related controls: AC-18, IA-3.

(15) *INFORMATION SYSTEM MONITORING | WIRELESS TO WIRELINE COMMUNICATIONS*

The organization employs an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wireline networks.

Supplemental Guidance: Related control: AC-18.

(16) *INFORMATION SYSTEM MONITORING | CORRELATE MONITORING INFORMATION*

The organization correlates information from monitoring tools employed throughout the information system.

Deleted: to achieve

Supplemental Guidance: Correlating information from different monitoring tools can provide a more comprehensive view of information system activity. The correlation of monitoring tools that usually work in isolation (e.g., host monitoring, network monitoring, anti-virus software) can provide an organization-wide view and in so doing, may reveal otherwise unseen attack patterns. Understanding the capabilities/limitations of diverse monitoring tools and how to maximize the utility of information generated by those tools can help organizations to build, operate, and maintain effective monitoring programs. Related control: AU-6.

Deleted: situational awareness

(17) *INFORMATION SYSTEM MONITORING | INTEGRATED SITUATIONAL AWARENESS*

The organization correlates information from monitoring physical, cyber, and supply chain activities to achieve integrated, organization-wide situational awareness.

Deleted: results

Supplemental Guidance: This control enhancement correlates monitoring information from a more diverse set of information sources to achieve integrated situational awareness. Integrated situational awareness from a combination of physical, cyber, and supply chain monitoring activities enhances the capability of organizations to more quickly detect sophisticated cyber 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 just the cyber domain. Such monitoring may help reveal attacks on organizations that are operating across multiple attack vectors. Related control: SA-12.

Deleted: Enhancement Supplemental Guidance:

Deleted: the organization

Deleted: the

(18) *INFORMATION SYSTEM MONITORING | ANALYZE TRAFFIC / COVERT EXFILTRATION*

The organization analyzes outbound communications traffic at the external boundary of the information system (i.e., system perimeter) and at [*Assignment: organization-defined interior points within the system (e.g., subsystems, subnetworks)*] to detect covert exfiltration of information.

Supplemental Guidance: Covert means that can be used for the unauthorized exfiltration of organizational information include, for example, steganography.

(19) *INFORMATION SYSTEM MONITORING | INDIVIDUALS POSING GREATER RISK*

The organization implements [*Assignment: organization-defined additional monitoring*] of individuals who have been identified by [*Assignment: organization-defined sources*] as posing an increased level of risk.

Supplemental Guidance: Indications of increased risk from individuals can be obtained from a variety of sources including, for example, human resource records, intelligence agencies, law enforcement organizations, and/or other credible sources. The monitoring of individuals is closely coordinated with management, legal, security, and human resources officials within organizations conducting such monitoring and complies with federal legislation, Executive Orders, policies, directives, regulations, and standards.

(20) *INFORMATION SYSTEM MONITORING | PRIVILEGED USER*

The organization implements [*Assignment: organization-defined additional monitoring*] of privileged users.

(21) *INFORMATION SYSTEM MONITORING | PROBATIONARY PERIODS*

The organization implements [*Assignment: organization-defined additional monitoring*] of individuals during [*Assignment: organization-defined probationary period*].

(22) *INFORMATION SYSTEM MONITORING | UNAUTHORIZED NETWORK SERVICES*

The information system detects network services that have not been authorized or approved by [*Assignment: organization-defined authorization or approval processes*] and [*Selection (one or more): audits; alerts* [*Assignment: organization-defined personnel or roles*]].

Supplemental Guidance: Unauthorized or unapproved network services include, for example, services in service-oriented architectures that lack organizational verification or validation and therefore may be unreliable or serve as malicious rogues for valid services. Related controls: AC-6, CM-7, SA-5, SA-9.

(23) *INFORMATION SYSTEM MONITORING | HOST-BASED DEVICES*

The organization implements [*Assignment: organization-defined host-based monitoring mechanisms*] at [*Assignment: organization-defined information system components*].

Supplemental Guidance: Information system components where host-based monitoring can be implemented include, for example, servers, workstations, and mobile devices. Organizations consider employing host-based monitoring mechanisms from multiple information technology product developers.

(24) *INFORMATION SYSTEM MONITORING | INDICATORS OF COMPROMISE*

The information system discovers, collects, distributes, and uses indicators of compromise.

Supplemental Guidance: Indicators of compromise (IOC) are forensic artifacts from intrusions that are identified on organizational information systems (at the host or network level). IOCs provide organizations with valuable information on objects or information systems that have been compromised. IOCs for the discovery of compromised hosts can include for example, the creation of registry key values. IOCs for network traffic include, for example, Universal Resource Locator (URL) or protocol elements that indicate malware command and control servers. The rapid distribution and adoption of IOCs can improve information security by reducing the time that information systems and organizations are vulnerable to the same exploit or attack.

References: NIST Special Publications 800-61, 800-83, 800-92, 800-94, 800-137.

Priority and Baseline Allocation:

P1	**LOW** SI-4	**MOD** SI-4 (2) (4) (5)	**HIGH** SI-4 (2) (4) (5)

Deleted: Not Selected

Deleted: (6)

Deleted: (6)

SI-5 SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

Control: The organization:

a. Receives information system security alerts, advisories, and directives from [*Assignment: organization-defined external organizations*] on an ongoing basis;

Deleted: designated

b. Generates internal security alerts, advisories, and directives as deemed necessary;

c. Disseminates security alerts, advisories, and directives to: [*Selection (one or more):* [*Assignment: organization-defined personnel or roles*]; [*Assignment: organization-defined elements within the organization*]; [*Assignment: organization-defined external organizations*]]; and

Deleted: *list of*

Deleted: *(identified by name and/or by role)*];

d. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

Supplemental Guidance: The United States Computer Emergency Readiness Team (US-CERT) generates security alerts and advisories to maintain situational awareness across the federal government. Security directives are issued by OMB or other designated organizations with the responsibility and authority to issue such directives. Compliance to security directives is essential due to the critical nature of many of these directives and the potential immediate adverse effects on organizational operations and assets, individuals, other organizations, and the Nation should the directives not be implemented in a timely manner. External organizations include, for example, external mission/business partners, supply chain partners, external service providers, and other peer/supporting organizations. Related control: SI-2.

Deleted: Security alerts and advisories are generated by the

Deleted:

Deleted:

Deleted: affects

Control Enhancements:

(1) *SECURITY ALERTS, ADVISORIES, AND DIRECTIVES | AUTOMATED ALERTS AND ADVISORIES*

The organization employs automated mechanisms to make security alert and advisory information available throughout the organization.

Deleted: as needed

Supplemental Guidance: The significant number of changes to organizational information 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 the information provided by the security alerts and advisories, changes may be required at one or more of the three tiers related to the management of information security risk including the governance level, mission/business process/enterprise architecture level, and the information system level.

References: NIST Special Publication 800-40.

Priority and Baseline Allocation:

P1	**LOW** SI-5	**MOD** SI-5	**HIGH** SI-5 (1)

SI-6 SECURITY FUNCTION VERIFICATION

Deleted: FUNCTIONALITY

Control: The information system:

Deleted: verifies

a. Verifies the correct operation of [*Assignment: organization-defined security functions*];

b. Performs this verification [*Selection (one or more):* [*Assignment: organization-defined system transitional states*]; *upon command by user with appropriate privilege;* [*Assignment: organization-defined frequency*]];

Deleted: *periodically every* [*Assignment: organization-defined time-period*]] and [*Selection (one or more): notifies system administrator; shuts the system down; restarts the system;* [*Assignment: organization-defined alternative action(s)*]] when anomalies are discovered.

c. Notifies [*Assignment: organization-defined personnel or roles*] of failed security verification tests; and

d. [*Selection (one or more): shuts the information system down; restarts the information system;* [*Assignment: organization-defined alternative action(s)*]] when anomalies are discovered.

Supplemental Guidance: Transitional states for information systems include, for example, system startup, restart, shutdown, and abort. Notifications provided by information systems include, for

Deleted: The need to verify security functionality applies to all security functions. For those security functions that are not able to execute automated self-tests, the organization either implements compensating security controls or explicitly accepts the risk of not performing the verification as required. Information system transitional example, electronic alerts to system administrators, messages to local computer consoles, and/or hardware indications such as lights. Related controls: CA-7, CM-6.

Control Enhancements:

(1) *SECURITY FUNCTION VERIFICATION | NOTIFICATION OF FAILED SECURITY TESTS*

[Withdrawn: Incorporated into SI-6].

(2) *SECURITY FUNCTION VERIFICATION | AUTOMATION SUPPORT FOR DISTRIBUTED TESTING*

The information system implements automated mechanisms to support for the management of distributed security testing.

Supplemental Guidance: Related control: SI-2.

(3) *SECURITY FUNCTION VERIFICATION | REPORT VERIFICATION RESULTS*

The organization reports the results of security function verification to *[Assignment: organization-defined personnel or roles]*.

Supplemental Guidance: Organizational personnel with potential interest in security function verification results include, for example, senior information security officers, information system security managers, and information systems security officers. Related controls: SA-12, SI-4, SI-5.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** Not Selected	**HIGH** SI-6

SI-7 SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY

Control: The organization employs integrity verification tools to detect unauthorized changes to *[Assignment: organization-defined software, firmware, and information]*.

Supplemental Guidance: Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity (e.g., tampering). Software includes, for example, operating systems (with key internal components such as kernels, drivers), middleware, and applications. Firmware includes, for example, the Basic Input Output System (BIOS). Information includes metadata such as security attributes associated with information. State-of-the-practice integrity-checking mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and associated tools can automatically monitor the integrity of information systems and hosted applications. Related controls: SA-12, SC-8, SC-13, SI-3.

Control Enhancements:

(1) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRITY CHECKS*

The information system performs an integrity check of *[Assignment: organization-defined software, firmware, and information]* [Selection (one or more): at startup; at [Assignment: organization-defined transitional states or security-relevant events]; [Assignment: organization-defined frequency]].

Supplemental Guidance: Security-relevant events include, for example, the identification of a new threat to which organizational information systems are susceptible, and the installation of new hardware, software, or firmware. Transitional states include, for example, system startup, restart, shutdown, and abort.

(2) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUTOMATED NOTIFICATIONS OF INTEGRITY VIOLATIONS*

The organization employs automated tools that provide notification to *[Assignment: organization-defined personnel or roles]* upon discovering discrepancies during integrity verification.

Supplemental Guidance: The use of automated tools to report integrity violations and to notify organizational personnel in a timely matter is an essential precursor to effective risk response. Personnel having an interest in integrity violations include, for example, mission/business

Deleted: The information system provides notification of failed automated security tests.

Deleted: provides

Deleted: result

Deleted: designated organizational officials with information security responsibilities.

Deleted: Enhancement

Deleted: officials

Deleted: information

Deleted: responsibilities

Deleted:

Deleted: information system detects

Deleted: .

Deleted: The organization employs integrity verification

Deleted: on

Deleted: system to look for evidence

Deleted: information tampering, errors, and omissions. The organization employs good software engineering practices with regard to commercial off

Deleted: shelf

Deleted: uses

Deleted: to

Deleted: the

Deleted: system

Deleted: the

Deleted: it hosts

Deleted: The organization reassesses the

Deleted: software and information by performing

Deleted:] integrity scans of the information system.

Deleted: designated individuals

owners, information system owners, systems administrators, software developers, systems integrators, and information security officers.

(3) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CENTRALLY-MANAGED INTEGRITY TOOLS*

The organization employs centrally managed integrity verification tools.

Supplemental Guidance: Related controls: AU-3, SI-2, SI-8.

(4) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | TAMPER-EVIDENT PACKAGING*

[Withdrawn: Incorporated into SA-12].

(5) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUTOMATED RESPONSE TO INTEGRITY VIOLATIONS*

Deleted: The organization requires use of tamper-evident packaging for [*Assignment: organization-defined information system components*] during [*Selection: transportation from vendor to operational site; during operation; both*].¶

The information system automatically [*Selection (one or more): shuts the information system down; restarts the information system; implements [Assignment: organization-defined security safeguards*]] when integrity violations are discovered.

Supplemental Guidance: Organizations may define different integrity checking and anomaly responses: (i) by type of information (e.g., firmware, software, user data); (ii) by specific information (e.g., boot firmware, boot firmware for a specific types of machines); or (iii) a combination of both. Automatic implementation of specific safeguards within organizational information systems includes, for example, reversing the changes, halting the information system, or triggering audit alerts when unauthorized modifications to critical security files occur.

(6) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CRYPTOGRAPHIC PROTECTION*

The information system implements cryptographic mechanisms to detect unauthorized changes to software, firmware, and information.

Supplemental Guidance: Cryptographic mechanisms used for the protection of integrity include, for example, digital signatures and the computation and application of signed hashes using asymmetric cryptography, protecting the confidentiality of the key used to generate the hash, and using the public key to verify the hash information. Related control: SC-13.

(7) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRATION OF DETECTION AND RESPONSE*

The organization incorporates the detection of unauthorized [*Assignment: organization-defined security-relevant changes to the information system*] into the organizational incident response capability.

Supplemental Guidance: This control enhancement helps to ensure that detected events are tracked, monitored, corrected, and available for historical purposes. Maintaining historical records is important both for being able to identify and discern adversary actions over an extended period of time and for possible legal actions. Security-relevant changes include, for example, unauthorized changes to established configuration settings or unauthorized elevation of information system privileges. Related controls: IR-4, IR-5, SI-4.

(8) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUDITING CAPABILITY FOR SIGNIFICANT EVENTS*

The information system, upon detection of a potential integrity violation, provides the capability to audit the event and initiates the following actions: [*Selection (one or more): generates an audit record; alerts current user; alerts [Assignment: organization-defined personnel or roles*]; [*Assignment: organization-defined other actions*]].

Supplemental Guidance: Organizations select response actions based on types of software, specific software, or information for which there are potential integrity violations. Related controls: AU-2, AU-6, AU-12.

(9) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | VERIFY BOOT PROCESS*

The information system verifies the integrity of the boot process of [*Assignment: organization-defined devices*].

Supplemental Guidance: Ensuring the integrity of boot processes is critical to starting devices in known/trustworthy states. Integrity verification mechanisms provide organizational personnel with assurance that only trusted code is executed during boot processes.

Deleted: [*Selection: transportation*

(10) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | PROTECTION OF BOOT FIRMWARE*

The information system implements [*Assignment: organization-defined security safeguards*] to protect the integrity of boot firmware in [*Assignment: organization-defined devices*].

Supplemental Guidance: Unauthorized modifications to boot firmware may be indicative of a sophisticated, targeted cyber attack. These types of cyber attacks can result in a permanent denial of service (e.g., if the firmware is corrupted) or a persistent malicious code presence (e.g., if code is embedded within the firmware). Devices can protect the integrity of the boot firmware in organizational information systems by: (i) verifying the integrity and authenticity of all updates to the boot firmware prior to applying changes to the boot devices; and (ii) preventing unauthorized processes from modifying the boot firmware.

(11) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CONFINED ENVIRONMENTS WITH LIMITED PRIVILEGES*

The organization requires that [*Assignment: organization-defined user-installed software*] execute in a confined physical or virtual machine environment with limited privileges.

Supplemental Guidance: Organizations identify software that may be of greater concern with regard to 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.

(12) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRITY VERIFICATION*

The organization requires that the integrity of [*Assignment: organization-defined user-installed software*] be verified prior to execution.

Supplemental Guidance: Organizations verify the integrity of user-installed software prior to execution to reduce the likelihood of executing malicious code or code that contains errors from unauthorized modifications. Organizations consider the practicality of approaches to verifying software integrity including, for example, availability of checksums of adequate trustworthiness from software developers or vendors.

(13) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CODE EXECUTION IN PROTECTED ENVIRONMENTS*

The organization allows execution of binary or machine-executable code obtained from sources with limited or no warranty and without the provision of source code only in confined physical or virtual machine environments and with the explicit approval of [*Assignment: organization-defined personnel or roles*].

Supplemental Guidance: This control enhancement applies to all sources of binary or machine-executable code including, for example, commercial software/firmware and open source software.

(14) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | BINARY OR MACHINE EXECUTABLE CODE*

The organization:

(a) Prohibits the use of binary or machine-executable code from sources with limited or no warranty and without the provision of source code; and

(b) Provides exceptions to the source code requirement only for compelling mission/operational requirements and with the approval of the authorizing official.

Supplemental Guidance: This control enhancement applies to all sources of binary or machine-executable code including, for example, commercial software/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 very difficult to review, repair, or extend, given that organizations, in most cases, do not have access to the original source code, and there may be no owners who could make such repairs on behalf of organizations. Related control: SA-5.

(15) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CODE AUTHENTICATION*

The information system implements cryptographic mechanisms to authenticate [*Assignment: organization-defined software or firmware components*] prior to installation.

Supplemental Guidance: Cryptographic authentication includes, for example, verifying that software or firmware components have been digitally signed using certificates recognized and approved by organizations. Code signing is an effective method to protect against malicious code.

(16) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | TIME LIMIT ON PROCESS EXECUTION W/O SUPERVISION*

The organization does not allow processes to execute without supervision for more than [*Assignment: organization-defined time period*].

Supplemental Guidance: This control enhancement addresses processes for which normal execution periods can be determined and situations in which organizations exceed such periods. Supervision includes, for example, operating system timers, automated responses, or manual oversight and response when information system process anomalies occur.

References: None.

References: NIST Special Publications 800-147, 800-155.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SI-7 (1) (7)	**HIGH** SI-7 (1) (2) (5) (7) (14)

SI-8 SPAM PROTECTION

Control: The organization:

a. Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and

b. Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

Deleted: and at workstations, servers, or mobile computing devices on the network

Deleted: transported by electronic mail, electronic mail attachments, web accesses, or other common means

Deleted: (including signature definitions)

Supplemental Guidance: Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, mobile devices, and notebook/laptop computers. Spam can be transported by different means including, for example, electronic mail, electronic mail attachments, and web accesses. Spam protection mechanisms include, for example, signature definitions. Related controls: AT-2, AT-3, SC-5, SC-7, SI-3.

Deleted: and

Deleted: .

Control Enhancements:

(1) *SPAM PROTECTION | CENTRAL MANAGEMENT*

The organization centrally manages spam protection mechanisms.

Supplemental Guidance: Central management is the organization-wide management and implementation of spam protection mechanisms. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed spam protection security controls. Related controls: AU-3, SI-2, SI-7.

(2) *SPAM PROTECTION | AUTOMATIC UPDATES*

The information system automatically updates spam protection mechanisms.

Deleted: (including signature definitions).

(3) *SPAM PROTECTION | CONTINUOUS LEARNING CAPABILITY*

The information system implements spam protection mechanisms with a learning capability to more effectively identify legitimate communications traffic.

Supplemental Guidance: Learning mechanisms include, for example, Bayesian filters that respond to user inputs identifying specific traffic as spam or legitimate by updating algorithm parameters and thereby more accurately separating types of traffic.

References: NIST Special Publication 800-45.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** SI-8 (1) (2)	**HIGH** SI-8 (1) (2)

Deleted: P1

SI-9 INFORMATION INPUT RESTRICTIONS

[Withdrawn: Incorporated into AC-2, AC-3, AC-5, AC-6].

SI-10 INFORMATION INPUT VALIDATION

Control: The information system checks the validity of [*Assignment: organization-defined information inputs*].

Supplemental Guidance: Checking the valid syntax and semantics of information system inputs (e.g., 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 tainted 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 helps to ensure accurate and correct inputs and prevent attacks such as cross-site scripting and a variety of injection attacks.

Control Enhancements:

(1) *INFORMATION INPUT VALIDATION | MANUAL OVERRIDE CAPABILITY*

The information system:

(a) Provides a manual override capability for input validation of [*Assignment: organization-defined inputs*];

(b) Restricts the use of the manual override capability to only [*Assignment: organization-defined authorized individuals*]; and

(c) Audits the use of the manual override capability.

Supplemental Guidance: Related controls: CM-3, CM-5.

(2) *INFORMATION INPUT VALIDATION | REVIEW / RESOLUTION OF ERRORS*

The organization ensures that input validation errors are reviewed and resolved within [*Assignment: organization-defined time period*].

Supplemental Guidance: Resolution of input validation errors includes, for example, correcting systemic causes of errors and resubmitting transactions with corrected input.

(3) *INFORMATION INPUT VALIDATION | PREDICTABLE BEHAVIOR*

The information system behaves in a predictable and documented manner that reflects organizational and system objectives when invalid inputs are received.

Supplemental Guidance: A common vulnerability in organizational information 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 information system responses that facilitate transitioning the system to known states without adverse, unintended side effects.

(4) *INFORMATION INPUT VALIDATION | REVIEW / TIMING INTERACTIONS*

The organization accounts for timing interactions among information system components in determining appropriate responses for invalid inputs.

Supplemental Guidance: In addressing invalid information system inputs received across protocol interfaces, timing interfaces 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

Deleted: Control: The organization restricts the capability to input information to the information system to authorized personnel.¶
Supplemental Guidance: Restrictions on organizational personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities. Related controls: AC-5, AC-6.¶
None.¶
P2 ...

Deleted: .

Deleted: Rules for checking

Deleted: are in place to verify

Deleted: Inputs passed

Deleted: are prescreened to prevent

Deleted: None.

precisely the wrong action in response to a collision event. Adversaries may be able to use apparently acceptable individual behaviors of the protocols in concert to achieve adverse effects through suitable construction of invalid input.

(5) INFORMATION INPUT VALIDATION | RESTRICT INPUTS TO TRUSTED SOURCES AND APPROVED FORMATS

The organization restricts the use of information inputs to [*Assignment: organization-defined trusted sources*] and/or [*Assignment: organization-defined formats*].

Supplemental Guidance: This control enhancement applies the concept of whitelisting to information inputs. Specifying known trusted sources for information inputs and acceptable formats for such inputs can reduce the probability of malicious activity.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SI-10	**HIGH** SI-10

SI-11 ERROR HANDLING

Control: The information system:

a. Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and

b. Reveals error messages only to [*Assignment: organization-defined* personnel *or roles*].

Deleted: <#>Identifies potentially security-relevant error conditions;¶

Deleted: [*Assignment: organization-defined sensitive or potentially harmful information*] in error logs and administrative messages

Deleted: authorized

Supplemental Guidance: Organizations carefully consider the structure/content of error messages. The extent to which information systems are able to identify and handle error conditions is guided by organizational policy and operational requirements. Information that could be exploited by adversaries 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) information recorded, and personal information such as account numbers, social security numbers, and credit card numbers. In addition, error messages may provide a covert channel for transmitting information. Related controls: AU-2, AU-3, SC-31.

Deleted: .

Deleted: The

Deleted: and

Deleted: are carefully considered by the organization.

Deleted: the

Deleted: system is

Deleted: Sensitive information

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** SI-11	**HIGH** SI-11

SI-12 INFORMATION HANDLING AND RETENTION

Deleted: OUTPUT

Control: The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

Deleted: both

Deleted: information

Supplemental Guidance: Information handling and retention requirements cover the full life cycle of information, in some cases extending beyond the disposal of information systems. The National Archives and Records Administration provides guidance on records retention. Related controls: AC-16, AU-5, AU-11, MP-2, MP-4.

Deleted: The output

Deleted: the

Deleted: the

Deleted: system.

Deleted:

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P2	**LOW** SI-12	**MOD** SI-12	**HIGH** SI-12

SI-13 PREDICTABLE FAILURE PREVENTION

Control: The organization:

a. Determines mean time to failure (MTTF) for [*Assignment: organization-defined information system components*] in specific environments of operation; and

b. Provides substitute information system components and a means to exchange active and standby components at [*Assignment: organization-defined MTTF substitution criteria*].

Supplemental Guidance: While MTTF is primarily a reliability issue, this control addresses potential failures of specific information system components that provide security capability. Failure rates reflect installation-specific consideration, not industry-average. Organizations define criteria for substitution of information system components based on 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 (e.g., preservation of state variables). Standby components remain available at all times except for maintenance issues or recovery failures in progress. Related controls: CP-2, CP-10, MA-6.

Control Enhancements:

(1) *PREDICTABLE FAILURE PREVENTION | TRANSFERRING COMPONENT RESPONSIBILITIES*

The organization takes information system components out of service by transferring component responsibilities to substitute components no later than [*Assignment: organization-defined fraction or percentage*] of mean time to failure.

(2) *PREDICTABLE FAILURE PREVENTION | TIME LIMIT ON PROCESS EXECUTION WITHOUT SUPERVISION*

[Withdrawn: Incorporated into SI-7 (16)].

(3) *PREDICTABLE FAILURE PREVENTION | MANUAL TRANSFER BETWEEN COMPONENTS*

The organization manually initiates transfers between active and standby information system components [*Assignment: organization-defined frequency*] if the mean time to failure exceeds [*Assignment: organization-defined time period*].

(4) *PREDICTABLE FAILURE PREVENTION | STANDBY COMPONENT INSTALLATION / NOTIFICATION*

The organization, if information system component failures are detected:

(a) **Ensures that the standby components are successfully and transparently installed within [*Assignment: organization-defined time period*]; and**

(b) **[*Selection (one or more): activates* [*Assignment: organization-defined alarm*]; *automatically shuts down the information system*].**

Supplemental Guidance: Automatic or manual transfer of components from standby to active mode can occur, for example, upon detection of component failures.

(5) *PREDICTABLE FAILURE PREVENTION | FAILOVER CAPABILITY*

The organization provides [*Selection: real-time; near real-time*] [*Assignment: organization-defined failover capability*] *for the information system.*

Supplemental Guidance: Failover refers to the automatic switchover to an alternate information system upon the failure of the primary information system. Failover capability includes, for example, incorporating mirrored information system operations at alternate processing sites or periodic data mirroring at regular intervals defined by recovery time periods of organizations.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

Deleted: Protects the information system from harm by considering

Deleted: *list of*

Deleted: , when needed,

Deleted: mechanism

Deleted: roles of the

Deleted: .

Deleted: mean time to failure

Deleted: focuses on the

Deleted: failure

Deleted: components of the

Deleted: Mean time to failure

Deleted: are defendable and based on considerations that are

Deleted: The transfer

Deleted: information system

Deleted: are preserved). The standby component is

Deleted: where a failure recovery is in progress or

Deleted: reasons.

Deleted: control

Deleted: the

Deleted: component

Deleted: a

Deleted: component

Deleted: The organization does not allow a process to execute without supervision for more than [*Assignment: organization-defined time period*].¶

Deleted: a transfer

Deleted: at least once per

Deleted: an

Deleted: failure is

Deleted: information system component

Deleted: assumes its role

Deleted: Enhancement

Deleted: roles to a

Deleted: unit may

Deleted: a

SI-14 NON-PERSISTENCE

Control: The organization implements non-persistent [*Assignment: organization-defined information system components and services*] that are initiated in a known state and terminated [*Selection (one or more): upon end of session of use; periodically at* [*Assignment: organization-defined frequency*]].

Supplemental Guidance: This control mitigates risk from advanced persistent threats (APTs) by significantly reducing the targeting capability of adversaries (i.e., window of opportunity and available attack surface) to initiate and complete cyber attacks. By implementing the concept of non-persistence for selected information system components, organizations can provide a known state computing resource for a specific period of time that does not give adversaries sufficient time on target to exploit vulnerabilities in organizational information systems and the environments in which those systems operate. Since the advanced persistent threat is a high-end threat with regard to capability, intent, and targeting, organizations assume that over an extended period of time, a percentage of cyber attacks will be successful. Non-persistent information system components and services are activated as required using protected information and terminated periodically or upon the end of sessions. Non-persistence increases the work factor of adversaries in attempting to compromise or breach organizational information systems.

Non-persistent system components can be implemented, 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 information system components/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 for organizations to determine). The refresh of selected information 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 information system unstable. In some instances, refreshes of critical components and services may be done periodically in order to hinder the ability of adversaries to exploit optimum windows of vulnerabilities. Related controls: SC-30, SC-34.

Control Enhancements:

(1) *NON-PERSISTENCE | REFRESH FROM TRUSTED SOURCES*

The organization ensures that software and data employed during information system component and service refreshes are obtained from [*Assignment: organization-defined trusted sources*].

Supplemental Guidance: Trusted sources include, for example, software/data from write-once, read-only media or from selected off-line secure storage facilities.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SI-15 INFORMATION OUTPUT FILTERING

Control: The information system validates information output from [*Assignment: organization-defined software programs and/or applications*] to ensure that the information is consistent with the expected content.

Supplemental Guidance: Certain types of cyber attacks (e.g., 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 alerting monitoring tools that anomalous behavior has been discovered. Related controls: SI-3, SI-4.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SI-16 MEMORY PROTECTION

Control: The information system implements [*Assignment: organization-defined security safeguards*] to protect its memory from unauthorized code execution.

Supplemental Guidance: Some adversaries launch attacks with the intent of executing code in non-executable regions of memory or in memory locations that are prohibited. Security safeguards employed to protect memory include, for example, data execution prevention and address space layout randomization. Data execution prevention safeguards can either be hardware-enforced or software-enforced with hardware providing the greater strength of mechanism. Related controls: AC-25, SC-3.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** SI-16	**HIGH** SI-16

SI-17 FAIL-SAFE PROCEDURES

Control: The information system implements [*Assignment: organization-defined fail-safe procedures*] when [*Assignment: organization-defined failure conditions occur*].

Supplemental Guidance: Failure conditions include, for example, loss of communications among critical system components or between system components and operational facilities. Fail-safe procedures include, for example, alerting operator personnel and providing specific instructions on subsequent steps to take (e.g., do nothing, reestablish system settings, shut down processes, restart the system, or contact designated organizational personnel). Related controls: CP-12, CP-13, SC-24, SI-13.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected