3.5 CONFIGURATION MANAGEMENT

Quick link to Configuration Management Summary Table

CM-1 POLICY AND PROCEDURES

Control:

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

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

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

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

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

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

c. Review and update the current configuration management:

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

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

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

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

Control Enhancements: None.

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

CM-2 BASELINE CONFIGURATION

Control:

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

b. Review and update the baseline configuration of the system:

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

2. When required due to [*Assignment: organization-defined circumstances*]; and

3. When system components are installed or upgraded.

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

Related Controls: AC-19, AU-6, CA-9, CM-1, CM-3, CM-5, CM-6, CM-8, CM-9, CP-9, CP-10, CP-12, MA-2, PL-8, PM-5, SA-8, SA-10, SA-15, SC-18.

Control Enhancements:

(1) BASELINE CONFIGURATION | REVIEWS AND UPDATES

[Withdrawn: Incorporated into CM-2.]

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

Maintain the currency, completeness, accuracy, and availability of the baseline configuration of the system using [*Assignment: organization-defined automated mechanisms*].

Discussion: Automated mechanisms that help organizations maintain consistent baseline configurations for systems include configuration management tools, hardware, software, firmware inventory tools, and network management tools. Automated tools can be used at the organization level, mission and business process level, or system level on workstations, servers, notebook computers, network components, or mobile devices. Tools can be used to track version numbers on operating systems, applications, types of software installed, and current patch levels. Automation support for accuracy and currency can be satisfied by the implementation of CM-8(2) for organizations that combine system component inventory and baseline configuration activities.

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

(3) BASELINE CONFIGURATION | RETENTION OF PREVIOUS CONFIGURATIONS

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

Discussion: Retaining previous versions of baseline configurations to support rollback include hardware, software, firmware, configuration files, configuration records, and associated documentation.

Related Controls: None.

(4) BASELINE CONFIGURATION | UNAUTHORIZED SOFTWARE

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

(5) BASELINE CONFIGURATION | AUTHORIZED SOFTWARE

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

(6) BASELINE CONFIGURATION | DEVELOPMENT AND TEST ENVIRONMENTS

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

Discussion: Establishing separate baseline configurations for development, testing, and operational environments protects systems from unplanned or 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, the management of operational configurations typically emphasizes the need for stability, while the management of development or test configurations requires greater flexibility. Configurations in the test environment mirror 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. Separate baseline configurations do not necessarily require separate physical environments.

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

(7) BASELINE CONFIGURATION | CONFIGURE SYSTEMS AND COMPONENTS FOR HIGH-RISK AREAS

(a) Issue [*Assignment: organization-defined systems or system components*] with [*Assignment: organization-defined configurations*] to individuals traveling to locations that the organization deems to be of significant risk; and

(b) Apply the following controls to the systems or components when the individuals return from travel: [*Assignment: organization-defined controls*].

Discussion: When it is known that systems or system components will be in high-risk areas external to the organization, additional controls may be implemented to counter the increased threat in such areas. For example, organizations can take actions for notebook computers used by individuals departing on and returning from travel. Actions include determining the locations that are of concern, defining the required configurations for the components, ensuring that components are configured as intended before travel is initiated, and applying controls to the components after travel is completed. Specially configured notebook computers include computers with sanitized hard drives, limited applications, and more stringent configuration settings. Controls applied to mobile devices upon return from travel include examining the mobile device for signs of physical tampering and purging and reimaging disk drives. Protecting information that resides on mobile devices is addressed in the MP (Media Protection) family.

Related Controls: MP-4, MP-5.

References: [SP 800-124], [SP 800-128].

CM-3 CONFIGURATION CHANGE CONTROL

Control:

a. Determine and document the types of changes to the system that are configuration-controlled;

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

c. Document configuration change decisions associated with the system;

d. Implement approved configuration-controlled changes to the system;

e. Retain records of configuration-controlled changes to the system for [*Assignment: organization-defined time period*];

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

g. Coordinate and provide oversight for configuration change control activities through [*Assignment: organization-defined configuration change control element*] that convenes [*Selection (one or more):* [*Assignment: organization-defined frequency*]; when [*Assignment: organization-defined configuration change conditions*]].

Discussion: Configuration change control for organizational systems involves the systematic proposal, justification, implementation, testing, review, and disposition of system changes, including system upgrades and modifications. Configuration change control includes changes to baseline configurations, configuration items of systems, operational procedures, configuration settings for system components, remediate vulnerabilities, and unscheduled or unauthorized changes. Processes for managing configuration changes to systems include Configuration Control Boards or Change Advisory Boards that review and approve proposed changes. For changes that impact privacy risk, the senior agency official for privacy updates privacy impact assessments and system of records notices. For new systems or major upgrades, organizations consider including representatives from the development organizations on the Configuration Control Boards or Change Advisory Boards. Auditing of changes includes activities before and after changes are made to systems and the auditing activities required to implement such changes. See also SA-10.

Related Controls: CA-7, CM-2, CM-4, CM-5, CM-6, CM-9, CM-11, IA-3, MA-2, PE-16, PT-6, RA-8, SA-8, SA-10, SC-28, SC-34, SC-37, SI-2, SI-3, SI-4, SI-7, SI-10, SR-11.

Control Enhancements:

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

Use [*Assignment: organization-defined automated mechanisms*] to:

(a) Document proposed changes to the system;

(b) Notify [*Assignment: organization-defined approval authorities*] of proposed changes to the system and request change approval;

(c) Highlight proposed changes to the system that have not been approved or disapproved within [*Assignment: organization-defined time period*];

(d) Prohibit changes to the system until designated approvals are received;

(e) Document all changes to the system; and

(f) Notify [*Assignment: organization-defined personnel*] when approved changes to the system are completed.

Discussion: None.

Related Controls: None.

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

Test, validate, and document changes to the system before finalizing the implementation of the changes.

Discussion: Changes to systems include modifications to hardware, software, or firmware components and configuration settings defined in CM-6. Organizations ensure that testing does not interfere with system operations that support organizational mission and business functions. Individuals or groups conducting tests understand security and privacy policies and procedures, system security and privacy policies and procedures, and the health, safety, and environmental risks associated with specific facilities or processes. Operational systems

may need to be taken offline, or replicated to the extent feasible, before testing can be conducted. If systems must be taken offline for testing, the tests are scheduled to occur during planned system outages whenever possible. If the testing cannot be conducted on operational systems, organizations employ compensating controls.

Related Controls: None.

(3) CONFIGURATION CHANGE CONTROL | AUTOMATED CHANGE IMPLEMENTATION

Implement changes to the current system baseline and deploy the updated baseline across the installed base using [*Assignment: organization-defined automated mechanisms*].

Discussion: Automated tools can improve the accuracy, consistency, and availability of configuration baseline information. Automation can also provide data aggregation and data correlation capabilities, alerting mechanisms, and dashboards to support risk-based decision-making within the organization.

Related Controls: None.

(4) CONFIGURATION CHANGE CONTROL | SECURITY AND PRIVACY REPRESENTATIVES

Require [*Assignment: organization-defined* security and privacy representatives] to be members of the [*Assignment: organization-defined configuration change control element*].

Discussion: Information security and privacy representatives include system security officers, senior agency information security officers, senior agency officials for privacy, or system privacy officers. Representation by personnel with information security and privacy expertise is important because changes to system configurations can have unintended side effects, some of which may be security- or privacy-relevant. Detecting such changes early in the process can help avoid unintended, negative consequences that could ultimately affect the security and privacy posture of systems. The configuration change control element referred to in the second organization-defined parameter reflects the change control elements defined by organizations in CM-3*g*.

Related Controls: None.

(5) CONFIGURATION CHANGE CONTROL | AUTOMATED SECURITY RESPONSE

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

Discussion: Automated security responses include halting selected system functions, halting system processing, and issuing alerts or notifications to organizational personnel when there is an unauthorized modification of a configuration item.

Related Controls: None.

(6) CONFIGURATION CHANGE CONTROL | CRYPTOGRAPHY MANAGEMENT

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

Discussion: The controls referenced in the control enhancement refer to security and privacy controls from the control catalog. Regardless of the cryptographic mechanisms employed, processes and procedures are in place to manage those mechanisms. For example, if system components use certificates for identification and authentication, a process is implemented to address the expiration of those certificates.

Related Controls: SC-12.

(7) CONFIGURATION CHANGE CONTROL | REVIEW SYSTEM CHANGES

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

Discussion: Indications that warrant a review of changes to the system and the specific circumstances justifying such reviews may be obtained from activities carried out by organizations during the configuration change process or continuous monitoring process.

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

(8) CONFIGURATION CHANGE CONTROL | PREVENT OR RESTRICT CONFIGURATION CHANGES

Prevent or restrict changes to the configuration of the system under the following circumstances: [*Assignment: organization-defined circumstances*].

Discussion: System configuration changes can adversely affect critical system security and privacy functionality. Change restrictions can be enforced through automated mechanisms.

Related Controls: None.

References: [SP 800-124], [SP 800-128], [IR 8062].

CM-4 IMPACT ANALYSES

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

Discussion: Organizational personnel with security or privacy responsibilities conduct impact analyses. Individuals conducting impact analyses possess the necessary skills and technical expertise to analyze the changes to systems as well as the security or privacy ramifications. Impact analyses include reviewing security and privacy plans, policies, and procedures to understand control requirements; reviewing system design documentation and operational procedures to understand control implementation and how specific system changes might affect the controls; reviewing the impact of changes on organizational supply chain partners with stakeholders; and determining how potential changes to a system create new risks to the privacy of individuals and the ability of implemented controls to mitigate those risks. Impact analyses also include risk assessments to understand the impact of the changes and determine if additional controls are required.

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

Control Enhancements:

(1) IMPACT ANALYSES | SEPARATE TEST ENVIRONMENTS

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

Discussion: A separate test environment requires an environment that is physically or logically separate 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 that 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 implemented, organizations determine the strength of mechanism required when implementing logical separation.

Related Controls: SA-11, SC-7.

(2) IMPACT ANALYSES | VERIFICATION OF CONTROLS

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

Discussion: Implementation in this context refers to installing changed code in the operational system that may have an impact on security or privacy controls.

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

References: [SP 800-128].

CM-5 ACCESS RESTRICTIONS FOR CHANGE

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

Discussion: Changes to the hardware, software, or firmware components of systems or the operational procedures related to the system can potentially have significant effects on the security of the systems or individuals' privacy. Therefore, organizations permit only qualified and authorized individuals to access systems for purposes of initiating changes. Access restrictions include physical and logical access controls (see AC-3 and PE-3), software libraries, workflow automation, media libraries, abstract layers (i.e., changes implemented into external interfaces rather than directly into systems), and change windows (i.e., changes occur only during specified times).

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

Control Enhancements:

(1) ACCESS RESTRICTIONS FOR CHANGE | AUTOMATED ACCESS ENFORCEMENT AND AUDIT RECORDS

(a) Enforce access restrictions using [*Assignment: organization-defined automated mechanisms*]; and

(b) Automatically generate audit records of the enforcement actions.

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

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

(2) ACCESS RESTRICTIONS FOR CHANGE | REVIEW SYSTEM CHANGES

[Withdrawn: Incorporated into CM-3(7).]

(3) ACCESS RESTRICTIONS FOR CHANGE | SIGNED COMPONENTS

[Withdrawn: Moved to CM-14.]

(4) ACCESS RESTRICTIONS FOR CHANGE | DUAL AUTHORIZATION

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

Discussion: Organizations employ dual authorization to help ensure that any changes to selected system components and information cannot occur unless two qualified individuals approve and implement such changes. The two individuals possess the skills and expertise to determine if the proposed changes are correct implementations of approved changes. The individuals are also accountable for the changes. Dual authorization may also be known as two-person control. To reduce the risk of collusion, organizations consider rotating dual authorization duties to other individuals. System-level information includes operational procedures.

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

(5) ACCESS RESTRICTIONS FOR CHANGE | PRIVILEGE LIMITATION FOR PRODUCTION AND OPERATION

(a) Limit privileges to change system components and system-related information within a production or operational environment; and

(b) Review and reevaluate privileges [*Assignment: organization-defined frequency*].

Discussion: In many organizations, systems support multiple mission and business functions. Limiting privileges to change system components with respect to operational systems is necessary because changes to a system component may have far-reaching effects on mission and business processes supported by the system. The relationships between systems and mission/business processes are, in some cases, unknown to developers. System-related information includes operational procedures.

Related Controls: AC-2.

(6) ACCESS RESTRICTIONS FOR CHANGE | LIMIT LIBRARY PRIVILEGES

Limit privileges to change software resident within software libraries.

Discussion: Software libraries include privileged programs.

Related Controls: AC-2.

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

[Withdrawn: Incorporated into SI-7.]

References: [FIPS 140-3]; [FIPS 186-4].

CM-6 CONFIGURATION SETTINGS

Control:

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

b. Implement the configuration settings;

c. Identify, document, and approve any deviations from established configuration settings for [*Assignment: organization-defined system components*] based on [*Assignment: organization-defined operational requirements*]; and

d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

Discussion: Configuration settings are the parameters that can be changed in the hardware, software, or firmware components of the system that affect the security and privacy posture or functionality of the system. Information technology products for which configuration settings can be defined include mainframe computers, servers, workstations, operating systems, mobile devices, input/output devices, protocols, and applications. Parameters that impact the security posture of systems include registry settings; account, file, or directory permission settings; and settings for functions, protocols, ports, services, and remote connections. Privacy parameters are parameters impacting the privacy posture of systems, including the parameters required to satisfy other privacy controls. Privacy parameters include settings for access controls, data processing preferences, and processing and retention permissions. Organizations establish organization-wide configuration settings and subsequently derive specific configuration settings for systems. The established settings become part of the configuration baseline for the system.

Common secure configurations (also known as security configuration checklists, lockdown and hardening guides, and security reference guides) provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for information technology

products and platforms as well as instructions for configuring those products or platforms to meet operational requirements. Common secure configurations can be developed by a variety of organizations, including information technology product developers, manufacturers, vendors, federal agencies, consortia, academia, industry, and other organizations in the public and private sectors.

Implementation of a common secure configuration may be mandated at the organization level, mission and business process level, system level, or at a higher level, including by a regulatory agency. Common secure configurations include the United States Government Configuration Baseline [USGCB] and security technical implementation guides (STIGs), which affect the implementation of CM-6 and other controls such as AC-19 and CM-7. The Security Content Automation Protocol (SCAP) and the defined standards within the protocol provide an effective method to uniquely identify, track, and control configuration settings.

Related Controls: AC-3, AC-19, AU-2, AU-6, CA-9, CM-2, CM-3, CM-5, CM-7, CM-11, CP-7, CP-9, CP-10, IA-3, IA-5, PL-8, PL-9, RA-5, SA-4, SA-5, SA-8, SA-9, SC-18, SC-28, SC-43, SI-2, SI-4, SI-6.

Control Enhancements:

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

Manage, apply, and verify configuration settings for [*Assignment: organization-defined system components*] using [*Assignment: organization-defined automated mechanisms*].

Discussion: Automated tools (e.g., hardening tools, baseline configuration tools) can improve the accuracy, consistency, and availability of configuration settings information. Automation can also provide data aggregation and data correlation capabilities, alerting mechanisms, and dashboards to support risk-based decision-making within the organization.

Related Controls: CA-7.

(2) CONFIGURATION SETTINGS | RESPOND TO UNAUTHORIZED CHANGES

Take the following actions in response to unauthorized changes to [*Assignment: organization-defined configuration settings*]: [*Assignment: organization-defined actions*].

Discussion: Responses to unauthorized changes to configuration settings include alerting designated organizational personnel, restoring established configuration settings, or—in extreme cases—halting affected system processing.

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

(3) CONFIGURATION SETTINGS | UNAUTHORIZED CHANGE DETECTION

[Withdrawn: Incorporated into SI-7.]

(4) CONFIGURATION SETTINGS | CONFORMANCE DEMONSTRATION

[Withdrawn: Incorporated into CM-4.]

References: [SP 800-70], [SP 800-126], [SP 800-128], [USGCB], [NCPR], [DOD STIG].

CM-7 LEAST FUNCTIONALITY

Control:

a. Configure the system to provide only [*Assignment: organization-defined mission essential capabilities*]; and

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

Discussion: Systems provide a wide variety of functions and services. Some of the functions and services routinely provided by default may not be necessary to support essential organizational missions, functions, or operations. Additionally, it is sometimes convenient to provide multiple services from a single system component, but doing so increases risk over limiting the services provided by that single component. Where feasible, organizations limit component functionality to a single function per component. Organizations consider removing unused or unnecessary software and disabling unused or unnecessary physical and logical ports and protocols to prevent unauthorized connection of components, transfer of information, and tunneling. Organizations employ network scanning tools, intrusion detection and prevention systems, and end-point protection technologies, such as firewalls and host-based intrusion detection systems, to identify and prevent the use of prohibited functions, protocols, ports, and services. Least functionality can also be achieved as part of the fundamental design and development of the system (see SA-8, SC-2, and SC-3).

Related Controls: AC-3, AC-4, CM-2, CM-5, CM-6, CM-11, RA-5, SA-4, SA-5, SA-8, SA-9, SA-15, SC-2, SC-3, SC-7, SC-37, SI-4.

Control Enhancements:

(1) LEAST FUNCTIONALITY | PERIODIC REVIEW

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

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

Discussion: Organizations review functions, ports, protocols, and services provided by systems or system components to determine the functions and services that are candidates for elimination. Such reviews are especially important during transition periods from older technologies to newer technologies (e.g., transition from IPv4 to IPv6). These technology transitions may require implementing the older and newer technologies simultaneously during the transition period and returning to minimum essential functions, ports, protocols, and services at the earliest opportunity. Organizations can either decide the relative security of the function, port, protocol, and/or service or base the security decision on the assessment of other entities. Unsecure protocols include Bluetooth, FTP, and peer-to-peer networking.

Related Controls: AC-18.

(2) LEAST FUNCTIONALITY | PREVENT PROGRAM EXECUTION

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

Discussion: Prevention of program execution addresses organizational policies, rules of behavior, and/or access agreements that restrict software usage and the terms and conditions imposed by the developer or manufacturer, including software licensing and copyrights. Restrictions include prohibiting auto-execute features, restricting roles allowed to approve program execution, permitting or prohibiting specific software programs, or restricting the number of program instances executed at the same time.

Related Controls: CM-8, PL-4, PL-9, PM-5, PS-6.

(3) LEAST FUNCTIONALITY | REGISTRATION COMPLIANCE

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

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

Related Controls: None.

(4) LEAST FUNCTIONALITY | UNAUTHORIZED SOFTWARE — DENY-BY-EXCEPTION

(a) Identify [*Assignment: organization-defined software programs not authorized to execute on the system*];

(b) Employ an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the system; and

(c) Review and update the list of unauthorized software programs [*Assignment: organization-defined frequency*].

Discussion: Unauthorized software programs can be limited to specific versions or from a specific source. The concept of prohibiting the execution of unauthorized software may also be applied to user actions, system ports and protocols, IP addresses/ranges, websites, and MAC addresses.

Related Controls: CM-6, CM-8, CM-10, PL-9, PM-5.

(5) LEAST FUNCTIONALITY | AUTHORIZED SOFTWARE — ALLOW-BY-EXCEPTION

(a) Identify [*Assignment: organization-defined software programs authorized to execute on the system*];

(b) Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system; and

(c) Review and update the list of authorized software programs [*Assignment: organization-defined frequency*].

Discussion: Authorized software programs can be limited to specific versions or from a specific source. To facilitate a comprehensive authorized software process and increase the strength of protection for attacks that bypass application level authorized software, software programs may be decomposed into and monitored at different levels of detail. These levels include applications, application programming interfaces, application modules, scripts, system processes, system services, kernel functions, registries, drivers, and dynamic link libraries. The concept of permitting the execution of authorized software may also be applied to user actions, system ports and protocols, IP addresses/ranges, websites, and MAC addresses. Organizations consider verifying the integrity of authorized software programs using digital signatures, cryptographic checksums, or hash functions. Verification of authorized software can occur either prior to execution or at system startup. The identification of authorized URLs for websites is addressed in CA-3(5) and SC-7.

Related Controls: CM-2, CM-6, CM-8, CM-10, PL-9, PM-5, SA-10, SC-34, SI-7.

(6) LEAST FUNCTIONALITY | CONFINED ENVIRONMENTS WITH LIMITED PRIVILEGES

Require that the following user-installed software execute in a confined physical or virtual machine environment with limited privileges: [*Assignment: organization-defined user-installed software*].

Discussion: Organizations identify software that may be of concern regarding its origin or potential for containing malicious code. For this type of software, user installations occur in confined environments of operation to limit or contain damage from malicious code that may be executed.

Related Controls: CM-11, SC-44.

(7) LEAST FUNCTIONALITY | CODE EXECUTION IN PROTECTED ENVIRONMENTS

Allow execution of binary or machine-executable code only in confined physical or virtual machine environments and with the explicit approval of [*Assignment: organization-defined personnel or roles*] when such code is:

(a) Obtained from sources with limited or no warranty; and/or

(b) Without the provision of source code.

Discussion: Code execution in protected environments applies to all sources of binary or machine-executable code, including commercial software and firmware and open-source software.

Related Controls: CM-10, SC-44.

(8) LEAST FUNCTIONALITY | BINARY OR MACHINE EXECUTABLE CODE

(a) Prohibit the use of binary or machine-executable code from sources with limited or no warranty or without the provision of source code; and

(b) Allow exceptions only for compelling mission or operational requirements and with the approval of the authorizing official.

Discussion: Binary or machine executable code applies to all sources of binary or machine-executable code, including commercial software and firmware and open-source software. Organizations assess software products without accompanying source code or from sources with limited or no warranty for potential security impacts. The assessments address the fact that software products without the provision of source code may be difficult to review, repair, or extend. In addition, there may be no owners to make such repairs on behalf of organizations. If open-source software is used, the assessments address the fact that there is no warranty, the open-source software could contain back doors or malware, and there may be no support available.

Related Controls: SA-5, SA-22.

(9) LEAST FUNCTIONALITY | PROHIBITING THE USE OF UNAUTHORIZED HARDWARE

(a) Identify [*Assignment: organization-defined hardware components authorized for system use*];

(b) Prohibit the use or connection of unauthorized hardware components;

(c) Review and update the list of authorized hardware components [*Assignment: organization-defined frequency*].

Discussion: Hardware components provide the foundation for organizational systems and the platform for the execution of authorized software programs. Managing the inventory of hardware components and controlling which hardware components are permitted to be installed or connected to organizational systems is essential in order to provide adequate security.

Related Controls: None.

References: [FIPS 140-3], [FIPS 180-4], [FIPS 186-4], [FIPS 202], [SP 800-167].

CM-8 SYSTEM COMPONENT INVENTORY

Control:

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

1. Accurately reflects the system;

2. Includes all components within the system;

3. Does not include duplicate accounting of components or components assigned to any other system;

4. Is at the level of granularity deemed necessary for tracking and reporting; and
5. Includes the following information to achieve system component accountability: [*Assignment: organization-defined information deemed necessary to achieve effective system component accountability*]; and

b. Review and update the system component inventory [*Assignment: organization-defined frequency*].

Discussion: System components are discrete, identifiable information technology assets that include hardware, software, and firmware. Organizations may choose to implement centralized system component inventories that include components from all organizational systems. In such situations, organizations ensure that the inventories include system-specific information required for component accountability. The information necessary for effective accountability of system components includes the system name, software owners, software version numbers, hardware inventory specifications, software license information, and for networked components, the machine names and network addresses across all implemented protocols (e.g., IPv4, IPv6). Inventory specifications include date of receipt, cost, model, serial number, manufacturer, supplier information, component type, and physical location.

Preventing duplicate accounting of system components addresses the lack of accountability that occurs when component ownership and system association is not known, especially in large or complex connected systems. Effective prevention of duplicate accounting of system components necessitates use of a unique identifier for each component. For software inventory, centrally managed software that is accessed via other systems is addressed as a component of the system on which it is installed and managed. Software installed on multiple organizational systems and managed at the system level is addressed for each individual system and may appear more than once in a centralized component inventory, necessitating a system association for each software instance in the centralized inventory to avoid duplicate accounting of components. Scanning systems implementing multiple network protocols (e.g., IPv4 and IPv6) can result in duplicate components being identified in different address spaces. The implementation of CM-8(7) can help to eliminate duplicate accounting of components.

Related Controls: CM-2, CM-7, CM-9, CM-10, CM-11, CM-13, CP-2, CP-9, MA-2, MA-6, PE-20, PL-9, PM-5, SA-4, SA-5, SI-2, SR-4.

Control Enhancements:

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

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

Discussion: Organizations can improve the accuracy, completeness, and consistency of system component inventories if the inventories are updated as part of component installations or removals or during general system updates. If inventories are not updated at these key times, there is a greater likelihood that the information will not be appropriately captured and documented. System updates include hardware, software, and firmware components.

Related Controls: PM-16.

(2) SYSTEM COMPONENT INVENTORY | AUTOMATED MAINTENANCE

Maintain the currency, completeness, accuracy, and availability of the inventory of system components using [*Assignment: organization-defined automated mechanisms*].

Discussion: Organizations maintain system inventories to the extent feasible. For example, virtual machines can be difficult to monitor because such machines are not visible to the network when not in use. In such cases, organizations maintain as up-to-date, complete, and

accurate an inventory as is deemed reasonable. Automated maintenance can be achieved by the implementation of CM-2(2) for organizations that combine system component inventory and baseline configuration activities.

Related Controls: None.

(3) SYSTEM COMPONENT INVENTORY | AUTOMATED UNAUTHORIZED COMPONENT DETECTION

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

(b) Take the following actions when unauthorized components are detected: [*Selection (one or more): disable network access by such components; isolate the components; notify* [*Assignment: organization-defined personnel or roles*]].

Discussion: Automated unauthorized component detection 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 may also be used to prevent the connection of unauthorized components (see CM-7(9)). Automated mechanisms can be implemented in systems or in separate system components. When acquiring and implementing automated mechanisms, organizations consider whether such mechanisms depend on the ability of the system component to support an agent or supplicant in order to be detected since some types of components do not have or cannot support agents (e.g., IoT devices, sensors). Isolation can be achieved , for example, by placing unauthorized system components in separate domains or subnets or quarantining such components. This type of component isolation is commonly referred to as "sandboxing."

Related Controls: AC-19, CA-7, RA-5, SC-3, SC-39, SC-44, SI-3, SI-4, SI-7.

(4) SYSTEM COMPONENT INVENTORY | ACCOUNTABILITY INFORMATION

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

Discussion: Identifying individuals who are responsible and accountable for administering system components ensures that the assigned components are properly administered and that organizations can contact those individuals if some action is required (e.g., when the component is determined to be the source of a breach, needs to be recalled or replaced, or needs to be relocated).

Related Controls: AC-3.

(5) SYSTEM COMPONENT INVENTORY | NO DUPLICATE ACCOUNTING OF COMPONENTS

[Withdrawn: Incorporated into CM-8.]

(6) SYSTEM COMPONENT INVENTORY | ASSESSED CONFIGURATIONS AND APPROVED DEVIATIONS

Include assessed component configurations and any approved deviations to current deployed configurations in the system component inventory.

Discussion: Assessed configurations and approved deviations focus on configuration settings established by organizations for system components, the specific components that have been assessed to determine compliance with the required configuration settings, and any approved deviations from established configuration settings.

Related Controls: None.

(7) SYSTEM COMPONENT INVENTORY | CENTRALIZED REPOSITORY

Provide a centralized repository for the inventory of system components.

Discussion: Organizations may implement centralized system component inventories that include components from all organizational systems. Centralized repositories of component inventories provide opportunities for efficiencies in accounting for organizational hardware, software, and firmware assets. Such repositories may also help organizations rapidly identify the location and responsible individuals of components that have been compromised, breached, or are otherwise in need of mitigation actions. Organizations ensure that the resulting centralized inventories include system-specific information required for proper component accountability.

Related Controls: None.

(8) SYSTEM COMPONENT INVENTORY | AUTOMATED LOCATION TRACKING

Support the tracking of system components by geographic location using [*Assignment: organization-defined automated mechanisms*].

Discussion: The use of automated mechanisms to track the location of system components can increase the accuracy of component inventories. Such capability may help organizations rapidly identify the location and responsible individuals of system components that have been compromised, breached, or are otherwise in need of mitigation actions. The use of tracking mechanisms can be coordinated with senior agency officials for privacy if there are implications that affect individual privacy.

Related Controls: None.

(9) SYSTEM COMPONENT INVENTORY | ASSIGNMENT OF COMPONENTS TO SYSTEMS

(a) Assign system components to a system; and

(b) Receive an acknowledgement from [*Assignment: organization-defined personnel or roles*] of this assignment.

Discussion: System components that are not assigned to a system may be unmanaged, lack the required protection, and become an organizational vulnerability.

Related Controls: None.

References: [OMB A-130], [SP 800-57-1], [SP 800-57-2], [SP 800-57-3], [SP 800-128], [IR 8011-2], [IR 8011-3].

CM-9 CONFIGURATION MANAGEMENT PLAN

Control: Develop, document, and implement a configuration management plan for the system that:

a. Addresses roles, responsibilities, and configuration management processes and procedures;

b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;

c. Defines the configuration items for the system and places the configuration items under configuration management;

d. Is reviewed and approved by [*Assignment: organization-defined personnel or roles*]; and

e. Protects the configuration management plan from unauthorized disclosure and modification.

Discussion: Configuration management activities occur throughout the system development life cycle. As such, there are developmental configuration management activities (e.g., the control of code and software libraries) and operational configuration management activities (e.g., control of installed components and how the components are configured). Configuration management plans satisfy the requirements in configuration management policies while being tailored to

individual systems. Configuration management plans define processes and procedures for how configuration management is used to support system development life cycle activities.

Configuration management plans are generated during the development and acquisition stage of the system development life cycle. The plans describe how to advance changes through change management processes; update configuration settings and baselines; maintain component inventories; control development, test, and operational environments; and develop, release, and update key documents.

Organizations can employ templates to help ensure the consistent and timely development and implementation of configuration management plans. Templates can represent a configuration management plan for the organization with subsets of the plan implemented on a system by system basis. Configuration management approval processes include the designation of key stakeholders responsible for reviewing and approving proposed changes to systems, and personnel who conduct security and privacy impact analyses prior to the implementation of changes to the systems. Configuration items are the system components, such as the hardware, software, firmware, and documentation to be configuration-managed. As systems continue through the system development life cycle, new configuration items may be identified, and some existing configuration items may no longer need to be under configuration control.

Related Controls: CM-2, CM-3, CM-4, CM-5, CM-8, PL-2, RA-8, SA-10, SI-12.

Control Enhancements:

(1) CONFIGURATION MANAGEMENT PLAN | ASSIGNMENT OF RESPONSIBILITY

Assign responsibility for developing the configuration management process to organizational personnel that are not directly involved in system development.

Discussion: In the absence of dedicated configuration management teams assigned within organizations, system developers may be tasked with developing configuration management processes using personnel who are not directly involved in system development or system integration. This separation of duties ensures that organizations establish and maintain a sufficient degree of independence between the system development and integration processes and configuration management processes to facilitate quality control and more effective oversight.

Related Controls: None.

References: [SP 800-128].

CM-10 SOFTWARE USAGE RESTRICTIONS

Control:

a. Use software and associated documentation in accordance with contract agreements and copyright laws;

b. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and

c. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

Discussion: Software license tracking can be accomplished by manual or automated methods, depending on organizational needs. Examples of contract agreements include software license agreements and non-disclosure agreements.

Related Controls: AC-17, AU-6, CM-7, CM-8, PM-30, SC-7.

Control Enhancements:

(1) SOFTWARE USAGE RESTRICTIONS | OPEN-SOURCE SOFTWARE

Establish the following restrictions on the use of open-source software: [*Assignment: organization-defined restrictions*].

Discussion: 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. In some cases, there is an online community associated with the software that inspects, tests, updates, and reports on issues found in software on an ongoing basis. However, remediating vulnerabilities in open-source software may be problematic. There may also be licensing issues associated with open-source software, including the constraints on derivative use of such software. Open-source software that is available only in binary form may increase the level of risk in using such software.

Related Controls: SI-7.

References: None.

CM-11 USER-INSTALLED SOFTWARE

Control:

a. Establish [*Assignment: organization-defined policies*] governing the installation of software by users;

b. Enforce software installation policies through the following methods: [*Assignment: organization-defined methods*]; and

c. Monitor policy compliance [*Assignment: organization-defined frequency*].

Discussion: If provided the necessary privileges, users can install software in organizational systems. To maintain control over the software installed, organizations identify permitted and prohibited actions regarding software installation. Permitted software installations include updates and security patches to existing software and downloading new applications from organization-approved "app stores." Prohibited software installations include software with unknown or suspect pedigrees or software that organizations consider potentially malicious. Policies selected for governing user-installed software are organization-developed or provided by some external entity. Policy enforcement methods can include procedural methods and automated methods.

Related Controls: AC-3, AU-6, CM-2, CM-3, CM-5, CM-6, CM-7, CM-8, PL-4, SI-4, SI-7.

Control Enhancements:

(1) USER-INSTALLED SOFTWARE | ALERTS FOR UNAUTHORIZED INSTALLATIONS

[Withdrawn: Incorporated into CM-8(3).]

(2) USER-INSTALLED SOFTWARE | SOFTWARE INSTALLATION WITH PRIVILEGED STATUS

Allow user installation of software only with explicit privileged status.

Discussion: Privileged status can be obtained, for example, by serving in the role of system administrator.

Related Controls: AC-5, AC-6.

(3) USER-INSTALLED SOFTWARE | AUTOMATED ENFORCEMENT AND MONITORING

Enforce and monitor compliance with software installation policies using [*Assignment: organization-defined automated mechanisms*].

Discussion: Organizations enforce and monitor compliance with software installation policies using automated mechanisms to more quickly detect and respond to unauthorized software installation which can be an indicator of an internal or external hostile attack.

Related Controls: None.

References: None.

CM-12 INFORMATION LOCATION

Control:

a. Identify and document the location of [*Assignment: organization-defined information*] and the specific system components on which the information is processed and stored;

b. Identify and document the users who have access to the system and system components where the information is processed and stored; and

c. Document changes to the location (i.e., system or system components) where the information is processed and stored.

Discussion: Information location addresses the need to understand where information is being processed and stored. Information location includes identifying where specific information types and information reside in system components and how information is being processed so that information flow can be understood and adequate protection and policy management provided for such information and system components. The security category of the information is also a factor in determining the controls necessary to protect the information and the system component where the information resides (see FIPS 199). The location of the information and system components is also a factor in the architecture and design of the system (see SA-4, SA-8, SA-17).

Related Controls: AC-2, AC-3, AC-4, AC-6, AC-23, CM-8, PM-5, RA-2, SA-4, SA-8, SA-17, SC-4, SC-16, SC-28, SI-4, SI-7.

Control Enhancements:

(1) INFORMATION LOCATION | AUTOMATED TOOLS TO SUPPORT INFORMATION LOCATION

Use automated tools to identify [*Assignment: organization-defined information by information type*] on [*Assignment: organization-defined system components*] to ensure controls are in place to protect organizational information and individual privacy.

Discussion: The use of automated tools helps to increase the effectiveness and efficiency of the information location capability implemented within the system. Automation also helps organizations manage the data produced during information location activities and share such information across the organization. The output of automated information location tools can be used to guide and inform system architecture and design decisions.

Related Controls: None.

References: [FIPS 199], [SP 800-60-1], [SP 800-60-2].

CM-13 DATA ACTION MAPPING

Control: Develop and document a map of system data actions.

Discussion: Data actions are system operations that process personally identifiable information. The processing of such information encompasses the full information life cycle, which includes collection, generation, transformation, use, disclosure, retention, and disposal. A map of system

data actions includes discrete data actions, elements of personally identifiable information being processed in the data actions, system components involved in the data actions, and the owners or operators of the system components. Understanding what personally identifiable information is being processed (e.g., the sensitivity of the personally identifiable information), how personally identifiable information is being processed (e.g., if the data action is visible to the individual or is processed in another part of the system), and by whom (e.g., individuals may have different privacy perceptions based on the entity that is processing the personally identifiable information) provides a number of contextual factors that are important to assessing the degree of privacy risk created by the system. Data maps can be illustrated in different ways, and the level of detail may vary based on the mission and business needs of the organization. The data map may be an overlay of any system design artifact that the organization is using. The development of this map may necessitate coordination between the privacy and security programs regarding the covered data actions and the components that are identified as part of the system.

Related Controls: AC-3, CM-4, CM-12, PM-5, PM-27, PT-2, PT-3, RA-3, RA-8.

CM-14 SIGNED COMPONENTS

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

Discussion: Software and firmware components prevented from installation unless signed with recognized and approved certificates include software and firmware version updates, patches, service packs, device drivers, and basic input/output system 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-12, SC-13, SI-7.

References: [IR 8062].