

3.4 ASSESSMENT, AUTHORIZATION, AND MONITORING

[Quick link to Assessment, Authorization, and Monitoring Summary Table](#)

CA-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*] assessment, authorization, and monitoring policy that:
 - (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 - (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
 2. Procedures to facilitate the implementation of the assessment, authorization, and monitoring policy and the associated assessment, authorization, and monitoring controls;
- b. Designate an [*Assignment: organization-defined official*] to manage the development, documentation, and dissemination of the assessment, authorization, and monitoring policy and procedures; and
- c. Review and update the current assessment, authorization, and monitoring:
 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: Assessment, authorization, and monitoring policy and procedures address the controls in the CA 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 assessment, authorization, and monitoring 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 or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to assessment, authorization, and monitoring policy and procedures include 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](#), [SI-12](#).

Control Enhancements: None.

References: [\[OMB A-130\]](#), [\[SP 800-12\]](#), [\[SP 800-30\]](#), [\[SP 800-37\]](#), [\[SP 800-39\]](#), [\[SP 800-53A\]](#), [\[SP 800-100\]](#), [\[SP 800-137\]](#), [\[SP 800-137A\]](#), [\[IR 8062\]](#).

CA-2 CONTROL ASSESSMENTS

Control:

- a. Select the appropriate assessor or assessment team for the type of assessment to be conducted;
- b. Develop a control assessment plan that describes the scope of the assessment including:
 1. Controls and control enhancements under assessment;
 2. Assessment procedures to be used to determine control effectiveness; and
 3. Assessment environment, assessment team, and assessment roles and responsibilities;
- c. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment;
- d. Assess the controls in the system and its environment of operation [*Assignment: organization-defined frequency*] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements;
- e. Produce a control assessment report that document the results of the assessment; and
- f. Provide the results of the control assessment to [*Assignment: organization-defined individuals or roles*].

Discussion: Organizations ensure that control assessors possess the required skills and technical expertise to develop effective assessment plans and to conduct assessments of system-specific, hybrid, common, and program management controls, as appropriate. The required skills include general knowledge of risk management concepts and approaches as well as comprehensive knowledge of and experience with the hardware, software, and firmware system components implemented.

Organizations assess controls in systems and the environments in which those systems operate as part of initial and ongoing authorizations, continuous monitoring, FISMA annual assessments, system design and development, systems security engineering, privacy engineering, and the system development life cycle. Assessments help to ensure that organizations meet information security and privacy requirements, identify weaknesses and deficiencies in the system design and development process, provide essential information needed to make risk-based decisions as part of authorization processes, and comply with vulnerability mitigation procedures. Organizations conduct assessments on the implemented controls as documented in security and privacy plans. Assessments can also be conducted throughout the system development life cycle as part of systems engineering and systems security engineering processes. The design for controls can be assessed as RFPs are developed, responses assessed, and design reviews conducted. If a design to implement controls and subsequent implementation in accordance with the design are assessed during development, the final control testing can be a simple confirmation utilizing previously completed control assessment and aggregating the outcomes.

Organizations may develop a single, consolidated security and privacy assessment plan for the system or maintain separate plans. A consolidated assessment plan clearly delineates the roles and responsibilities for control assessment. If multiple organizations participate in assessing a system, a coordinated approach can reduce redundancies and associated costs.

Organizations can use other types of assessment activities, such as vulnerability scanning and system monitoring, to maintain the security and privacy posture of systems during the system

life cycle. Assessment reports document assessment results in sufficient detail, as deemed necessary by organizations, to determine the accuracy and completeness of the reports and whether the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting requirements. Assessment results are provided to the individuals or roles appropriate for the types of assessments being conducted. For example, assessments conducted in support of authorization decisions are provided to authorizing officials, senior agency officials for privacy, senior agency information security officers, and authorizing official designated representatives.

To satisfy annual assessment requirements, organizations can use assessment results from the following sources: initial or ongoing system authorizations, continuous monitoring, systems engineering processes, or system development life cycle activities. Organizations ensure that assessment results are current, relevant to the determination of control effectiveness, and obtained with the appropriate level of assessor independence. Existing control assessment results can be reused to the extent that the results are still valid and can also be supplemented with additional assessments as needed. After the initial authorizations, organizations assess controls during continuous monitoring. Organizations also establish the frequency for ongoing assessments in accordance with organizational continuous monitoring strategies. External audits, including audits by external entities such as regulatory agencies, are outside of the scope of [CA-2](#).

Related Controls: [AC-20](#), [CA-5](#), [CA-6](#), [CA-7](#), [PM-9](#), [RA-5](#), [RA-10](#), [SA-11](#), [SC-38](#), [SI-3](#), [SI-12](#), [SR-2](#), [SR-3](#).

Control Enhancements:

(1) CONTROL ASSESSMENTS | [INDEPENDENT ASSESSORS](#)

Employ independent assessors or assessment teams to conduct control assessments.

Discussion: Independent assessors or assessment teams are individuals or groups who conduct impartial assessments of systems. Impartiality means that assessors are free from any perceived or actual conflicts of interest regarding the development, operation, sustainment, or management of the systems under assessment or the determination of control effectiveness. To achieve impartiality, assessors do not create a mutual or conflicting interest with the organizations where the assessments are being conducted, assess their own work, act as management or employees of the organizations they are serving, or place themselves in positions of advocacy for the organizations acquiring their services.

Independent assessments can be obtained from elements within organizations or be contracted to public or private sector entities outside of organizations. Authorizing officials determine the required level of independence based on the security categories of systems and/or the risk to organizational operations, organizational assets, or individuals. Authorizing officials also determine if the level of assessor independence provides sufficient assurance that the results are sound and can be used to make credible, risk-based decisions. Assessor independence determination includes whether contracted assessment services have sufficient independence, such as when system owners are not directly involved in contracting processes or cannot influence the impartiality of the assessors conducting the assessments. During the system design and development phase, having independent assessors is analogous to having independent SMEs involved in design reviews.

When organizations that own the systems are small or the structures of the organizations require that assessments be conducted by individuals that are in the developmental, operational, or management chain of the 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. Assessments performed for purposes other than to support

authorization decisions are more likely to be useable for such decisions when performed by assessors with sufficient independence, thereby reducing the need to repeat assessments.

Related Controls: None.

(2) CONTROL ASSESSMENTS | [SPECIALIZED ASSESSMENTS](#)

Include as part of control assessments, [Assignment: organization-defined frequency], [Selection: announced; unannounced], [Selection (one or more): in-depth monitoring; security instrumentation; automated security test cases; vulnerability scanning; malicious user testing; insider threat assessment; performance and load testing; data leakage or data loss assessment; [Assignment: organization-defined other forms of assessment]].

Discussion: Organizations can conduct specialized assessments, including verification and validation, system monitoring, insider threat assessments, malicious user testing, and other forms of testing. These assessments can improve readiness by exercising organizational capabilities and indicating current levels of performance as a means of focusing actions to improve security and privacy. Organizations conduct specialized assessments in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Authorizing officials approve the assessment methods in coordination with the organizational risk executive function. Organizations can include vulnerabilities uncovered during assessments into vulnerability remediation processes. Specialized assessments can also be conducted early in the system development life cycle (e.g., during initial design, development, and unit testing).

Related Controls: [PE-3](#), [SI-2](#).

(3) CONTROL ASSESSMENTS | [LEVERAGING RESULTS FROM EXTERNAL ORGANIZATIONS](#)

Leverage the results of control assessments performed by [Assignment: organization-defined external organization] on [Assignment: organization-defined system] when the assessment meets [Assignment: organization-defined requirements].

Discussion: Organizations may rely on control assessments of organizational systems by other (external) organizations. Using such assessments and reusing existing assessment evidence can decrease the time and resources required for assessments by limiting the independent assessment activities that organizations need to perform. The factors that organizations consider in determining whether to accept assessment results from external organizations can vary. Such factors include the organization's past experience with the organization that conducted the assessment, the reputation of the assessment organization, the level of detail of supporting assessment evidence provided, and mandates imposed by applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Accredited testing laboratories that support the Common Criteria Program ([ISO 15408-1](#)), the NIST Cryptographic Module Validation Program (CMVP), or the NIST Cryptographic Algorithm Validation Program (CAVP) can provide independent assessment results that organizations can leverage.

Related Controls: [SA-4](#).

References: [\[OMB A-130\]](#), [\[FIPS 199\]](#), [\[SP 800-18\]](#), [\[SP 800-37\]](#), [\[SP 800-39\]](#), [\[SP 800-53A\]](#), [\[SP 800-115\]](#), [\[SP 800-137\]](#), [\[IR 8011-1\]](#), [\[IR 8062\]](#).

[CA-3](#) INFORMATION EXCHANGE

Control:

- a. Approve and manage the exchange of information between the system and other systems using [Selection (one or more): interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service level agreements;

user agreements; nondisclosure agreements; [Assignment: organization-defined type of agreement]]];

- b. Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated; and
- c. Review and update the agreements [*Assignment: organization-defined frequency*].

Discussion: System information exchange requirements apply to information exchanges between two or more systems. System information exchanges include connections via leased lines or virtual private networks, connections to internet service providers, database sharing or exchanges of database transaction information, connections and exchanges with cloud services, exchanges via web-based services, or exchanges of files via file transfer protocols, network protocols (e.g., IPv4, IPv6), email, or other organization-to-organization communications. Organizations consider the risk related to new or increased threats that may be introduced when systems exchange information with other systems that may have different security and privacy requirements and controls. This includes systems within the same organization and systems that are external to the organization. A joint authorization of the systems exchanging information, as described in [CA-6\(1\)](#) or [CA-6\(2\)](#), may help to communicate and reduce risk.

Authorizing officials determine the risk associated with system information exchange and the controls needed for appropriate risk mitigation. The types of agreements selected are based on factors such as the impact level of the information being exchanged, the relationship between the organizations exchanging information (e.g., government to government, government to business, business to business, government or business to service provider, government or business to individual), or the level of access to the organizational system by users of the other system. If systems that exchange information have the same authorizing official, organizations need not develop agreements. Instead, the interface characteristics between the systems (e.g., how the information is being exchanged, how the information is protected) are described in the respective security and privacy plans. If the systems that exchange information have different authorizing officials within the same organization, the organizations can develop agreements or provide the same information that would be provided in the appropriate agreement type from [CA-3a](#) in the respective security and privacy plans for the systems. Organizations may incorporate agreement information into formal contracts, especially for information exchanges established between federal agencies and nonfederal organizations (including service providers, contractors, system developers, and system integrators). Risk considerations include systems that share the same networks.

Related Controls: [AC-4](#), [AC-20](#), [AU-16](#), [CA-6](#), [IA-3](#), [IR-4](#), [PL-2](#), [PT-7](#), [RA-3](#), [SA-9](#), [SC-7](#), [SI-12](#).

Control Enhancements:

- (1) SYSTEM CONNECTIONS | UNCLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS
[Withdrawn: Moved to [SC-7\(25\)](#).]
- (2) SYSTEM CONNECTIONS | CLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS
[Withdrawn: Moved to [SC-7\(26\)](#).]
- (3) SYSTEM CONNECTIONS | UNCLASSIFIED NON-NATIONAL SECURITY SYSTEM CONNECTIONS
[Withdrawn: Moved to [SC-7\(27\)](#).]
- (4) SYSTEM CONNECTIONS | CONNECTIONS TO PUBLIC NETWORKS
[Withdrawn: Moved to [SC-7\(28\)](#).]
- (5) SYSTEM CONNECTIONS | RESTRICTIONS ON EXTERNAL SYSTEM CONNECTIONS

[Withdrawn: Moved to [SC-7\(5\)](#).]

(6) INFORMATION EXCHANGE | [TRANSFER AUTHORIZATIONS](#)

Verify that individuals or systems transferring data between interconnecting systems have the requisite authorizations (i.e., write permissions or privileges) prior to accepting such data.

Discussion: To prevent unauthorized individuals and systems from making information transfers to protected systems, the protected system verifies—via independent means—whether the individual or system attempting to transfer information is authorized to do so. Verification of the authorization to transfer information also applies to control plane traffic (e.g., routing and DNS) and services (e.g., authenticated SMTP relays).

Related Controls: [AC-2](#), [AC-3](#), [AC-4](#).

(7) INFORMATION EXCHANGE | [TRANSITIVE INFORMATION EXCHANGES](#)

- (a) Identify transitive (downstream) information exchanges with other systems through the systems identified in [CA-3a](#); and**
- (b) Take measures to ensure that transitive (downstream) information exchanges cease when the controls on identified transitive (downstream) systems cannot be verified or validated.**

Discussion: Transitive or “downstream” information exchanges are information exchanges between the system or systems with which the organizational system exchanges information and other systems. For mission-essential systems, services, and applications, including high value assets, it is necessary to identify such information exchanges. The transparency of the controls or protection measures in place in such downstream systems connected directly or indirectly to organizational systems is essential to understanding the security and privacy risks resulting from those information exchanges. Organizational systems can inherit risk from downstream systems through transitive connections and information exchanges, which can make the organizational systems more susceptible to threats, hazards, and adverse impacts.

Related Controls: [SC-7](#).

References: [\[OMB A-130\]](#), [\[FIPS 199\]](#), [\[SP 800-47\]](#).

CA-4 SECURITY CERTIFICATION

[Withdrawn: Incorporated into [CA-2](#).]

[CA-5](#) PLAN OF ACTION AND MILESTONES

Control:

- a. Develop a plan of action and milestones for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and
- b. Update existing plan of action and milestones [*Assignment: organization-defined frequency*] based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities.

Discussion: Plans of action and milestones are useful for any type of organization to track planned remedial actions. Plans of action and milestones are required in authorization packages and subject to federal reporting requirements established by OMB.

Related Controls: [CA-2](#), [CA-7](#), [PM-4](#), [PM-9](#), [RA-7](#), [SI-2](#), [SI-12](#).

Control Enhancements:**(1) PLAN OF ACTION AND MILESTONES | [AUTOMATION SUPPORT FOR ACCURACY AND CURRENCY](#)**

Ensure the accuracy, currency, and availability of the plan of action and milestones for the system using [Assignment: organization-defined automated mechanisms].

Discussion: Using automated tools helps maintain the accuracy, currency, and availability of the plan of action and milestones and facilitates the coordination and sharing of security and privacy information throughout the organization. Such coordination and information sharing help to identify systemic weaknesses or deficiencies in organizational systems and ensure that appropriate resources are directed at the most critical system vulnerabilities in a timely manner.

Related Controls: None.

References: [\[OMB A-130\]](#), [\[SP 800-37\]](#).

CA-6 AUTHORIZATIONControl:

- a. Assign a senior official as the authorizing official for the system;
- b. Assign a senior official as the authorizing official for common controls available for inheritance by organizational systems;
- c. Ensure that the authorizing official for the system, before commencing operations:
 1. Accepts the use of common controls inherited by the system; and
 2. Authorizes the system to operate;
- d. Ensure that the authorizing official for common controls authorizes the use of those controls for inheritance by organizational systems;
- e. Update the authorizations [Assignment: organization-defined frequency].

Discussion: Authorizations are official management decisions by senior officials to authorize operation of systems, authorize the use of common controls for inheritance by organizational systems, and explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of agreed-upon controls. Authorizing officials provide budgetary oversight for organizational systems and common controls or assume responsibility for the mission and business functions supported by those systems or common controls. The authorization process is a federal responsibility, and therefore, authorizing officials must be federal employees. Authorizing officials are both responsible and accountable for security and privacy risks associated with the operation and use of organizational systems. Nonfederal organizations may have similar processes to authorize systems and senior officials that assume the authorization role and associated responsibilities.

Authorizing officials issue ongoing authorizations of systems based on evidence produced from implemented continuous monitoring programs. Robust continuous monitoring programs reduce the need for separate reauthorization processes. Through the employment of comprehensive continuous monitoring processes, the information contained in authorization packages (i.e., security and privacy plans, assessment reports, and plans of action and milestones) is updated on an ongoing basis. This provides authorizing officials, common control providers, and system owners with an up-to-date status of the security and privacy posture of their systems, controls, and operating environments. To reduce the cost of reauthorization, authorizing officials can leverage the results of continuous monitoring processes to the maximum extent possible as the basis for rendering reauthorization decisions.

Related Controls: [CA-2](#), [CA-3](#), [CA-7](#), [PM-9](#), [PM-10](#), [RA-3](#), [SA-10](#), [SI-12](#).

Control Enhancements:

(1) AUTHORIZATION | [JOINT AUTHORIZATION — INTRA-ORGANIZATION](#)

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

Discussion: Assigning multiple authorizing officials from the same organization to serve as co-authorizing officials for the system increases the level of independence in the risk-based decision-making process. It also implements the concepts of separation of duties and dual authorization as applied to the system authorization process. The intra-organization joint authorization process is most relevant for connected systems, shared systems, and systems with multiple information owners.

Related Controls: [AC-6](#).

(2) AUTHORIZATION | [JOINT AUTHORIZATION — INTER-ORGANIZATION](#)

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

Discussion: Assigning multiple authorizing officials, at least one of whom comes from an external organization, to serve as co-authorizing officials for the system increases the level of independence in the risk-based decision-making process. It implements the concepts of separation of duties and dual authorization as applied to the system authorization process. Employing authorizing officials from external organizations to supplement the authorizing official from the organization that owns or hosts the system may be necessary when the external organizations have a vested interest or equities in the outcome of the authorization decision. The inter-organization joint authorization process is relevant and appropriate for connected systems, shared systems or services, and systems with multiple information owners. The authorizing officials from the external organizations are key stakeholders of the system undergoing authorization.

Related Controls: [AC-6](#).

References: [\[OMB A-130\]](#), [\[SP 800-37\]](#), [\[SP 800-137\]](#).

[CA-7](#) CONTINUOUS MONITORING

Control: Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes:

- a. Establishing the following system-level metrics to be monitored: *[Assignment: organization-defined system-level metrics]*;
- b. Establishing *[Assignment: organization-defined frequencies]* for monitoring and *[Assignment: organization-defined frequencies]* for assessment of control effectiveness;
- c. Ongoing control assessments in accordance with the continuous monitoring strategy;
- d. Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy;
- e. Correlation and analysis of information generated by control assessments and monitoring;
- f. Response actions to address results of the analysis of control assessment and monitoring information; and

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

Discussion: Continuous monitoring at the system level facilitates ongoing awareness of the system security and privacy posture to support organizational risk management decisions. The terms “continuous” and “ongoing” imply that organizations assess and monitor their controls and risks at a frequency sufficient to support risk-based decisions. Different types of controls may require different monitoring frequencies. The results of continuous monitoring generate risk response actions by organizations. When monitoring the effectiveness of multiple controls that have been grouped into capabilities, a root-cause analysis may be needed to determine the specific control that has failed. Continuous monitoring programs allow organizations to maintain the authorizations of systems and common controls in highly dynamic environments of operation with changing mission and business needs, threats, vulnerabilities, and technologies. Having access to security and privacy information on a continuing basis through reports and dashboards gives organizational officials the ability to make effective and timely risk management decisions, including ongoing authorization decisions.

Automation supports more frequent updates to hardware, software, and firmware inventories, authorization packages, and other system information. Effectiveness is further enhanced when continuous monitoring outputs are formatted to provide information that is specific, measurable, actionable, relevant, and timely. Continuous monitoring activities are scaled in accordance with the security categories of systems. Monitoring requirements, including the need for specific monitoring, may be referenced in other controls and control enhancements, such as [AC-2g](#), [AC-2\(7\)](#), [AC-2\(12\)\(a\)](#), [AC-2\(7\)\(b\)](#), [AC-2\(7\)\(c\)](#), [AC-17\(1\)](#), [AT-4a](#), [AU-13](#), [AU-13\(1\)](#), [AU-13\(2\)](#), [CM-3f](#), [CM-6d](#), [CM-11c](#), [IR-5](#), [MA-2b](#), [MA-3a](#), [MA-4a](#), [PE-3d](#), [PE-6](#), [PE-14b](#), [PE-16](#), [PE-20](#), [PM-6](#), [PM-23](#), [PM-31](#), [PS-7e](#), [SA-9c](#), [SR-4](#), [SC-5\(3\)\(b\)](#), [SC-7a](#), [SC-7\(24\)\(b\)](#), [SC-18b](#), [SC-43b](#), and [SI-4](#).

Related Controls: [AC-2](#), [AC-6](#), [AC-17](#), [AT-4](#), [AU-6](#), [AU-13](#), [CA-2](#), [CA-5](#), [CA-6](#), [CM-3](#), [CM-4](#), [CM-6](#), [CM-11](#), [IA-5](#), [IR-5](#), [MA-2](#), [MA-3](#), [MA-4](#), [PE-3](#), [PE-6](#), [PE-14](#), [PE-16](#), [PE-20](#), [PL-2](#), [PM-4](#), [PM-6](#), [PM-9](#), [PM-10](#), [PM-12](#), [PM-14](#), [PM-23](#), [PM-28](#), [PM-31](#), [PS-7](#), [PT-7](#), [RA-3](#), [RA-5](#), [RA-7](#), [RA-10](#), [SA-8](#), [SA-9](#), [SA-11](#), [SC-5](#), [SC-7](#), [SC-18](#), [SC-38](#), [SC-43](#), [SI-3](#), [SI-4](#), [SI-12](#), [SR-6](#).

Control Enhancements:

(1) CONTINUOUS MONITORING | [INDEPENDENT ASSESSMENT](#)

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

Discussion: Organizations maximize the value of control assessments by requiring that assessments be conducted by assessors with appropriate levels of independence. The level of required independence is based on organizational continuous monitoring strategies. Assessor independence provides a degree of impartiality to the monitoring process. To achieve such impartiality, assessors do not create a mutual or conflicting interest with the organizations where the assessments are being conducted, assess their own work, act as management or employees of the organizations they are serving, or place themselves in advocacy positions for the organizations acquiring their services.

Related Controls: None.

(2) CONTINUOUS MONITORING | TYPES OF ASSESSMENTS

[Withdrawn: Incorporated into [CA-2](#).]

(3) CONTINUOUS MONITORING | [TREND ANALYSES](#)

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

Discussion: Trend analyses include examining recent threat information that addresses the types of threat events that have occurred in the organization or the Federal Government, success rates of certain types of attacks, emerging vulnerabilities in technologies, evolving social engineering techniques, the effectiveness of configuration settings, results from multiple control assessments, and findings from Inspectors General or auditors.

Related Controls: None.

(4) CONTINUOUS MONITORING | [RISK MONITORING](#)

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

- (a) **Effectiveness monitoring;**
- (b) **Compliance monitoring; and**
- (c) **Change monitoring.**

Discussion: Risk monitoring is informed by the established organizational risk tolerance. Effectiveness monitoring determines the ongoing effectiveness of the implemented risk response measures. Compliance monitoring verifies that required risk response measures are implemented. It also verifies that security and privacy requirements are satisfied. Change monitoring identifies changes to organizational systems and environments of operation that may affect security and privacy risk.

Related Controls: None.

(5) CONTINUOUS MONITORING | [CONSISTENCY ANALYSIS](#)

Employ the following actions to validate that policies are established and implemented controls are operating in a consistent manner: [Assignment: organization-defined actions].

Discussion: Security and privacy controls are often added incrementally to a system. As a result, policies for selecting and implementing controls may be inconsistent, and the controls could fail to work together in a consistent or coordinated manner. At a minimum, the lack of consistency and coordination could mean that there are unacceptable security and privacy gaps in the system. At worst, it could mean that some of the controls implemented in one location or by one component are actually impeding the functionality of other controls (e.g., encrypting internal network traffic can impede monitoring). In other situations, failing to consistently monitor all implemented network protocols (e.g., a dual stack of IPv4 and IPv6) may create unintended vulnerabilities in the system that could be exploited by adversaries. It is important to validate—through testing, monitoring, and analysis—that the implemented controls are operating in a consistent, coordinated, non-interfering manner.

Related Controls: None.

(6) CONTINUOUS MONITORING | [AUTOMATION SUPPORT FOR MONITORING](#)

Ensure the accuracy, currency, and availability of monitoring results for the system using [Assignment: organization-defined automated mechanisms].

Discussion: Using automated tools for monitoring helps to maintain the accuracy, currency, and availability of monitoring information which in turns helps to increase the level of ongoing awareness of the system security and privacy posture in support of organizational risk management decisions.

Related Controls: None.

References: [\[OMB A-130\]](#), [\[SP 800-37\]](#), [\[SP 800-39\]](#), [\[SP 800-53A\]](#), [\[SP 800-115\]](#), [\[SP 800-137\]](#), [\[IR 8011-1\]](#), [\[IR 8062\]](#).

CA-8 PENETRATION TESTING

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

Discussion: Penetration testing is a specialized type of assessment conducted on systems or individual system components to identify vulnerabilities that could be exploited by adversaries. Penetration testing goes beyond automated vulnerability scanning and is conducted by agents and teams with demonstrable skills and experience that include technical expertise in network, operating system, and/or application level security. Penetration testing can be used to validate vulnerabilities or determine the degree of penetration resistance of systems to adversaries within specified constraints. Such constraints include time, resources, and skills. Penetration testing attempts to duplicate the actions of adversaries and provides a more in-depth analysis of security- and privacy-related weaknesses or deficiencies. Penetration testing is especially important when organizations are transitioning from older technologies to newer technologies (e.g., transitioning from IPv4 to IPv6 network protocols).

Organizations can use the results of vulnerability analyses to support penetration testing activities. Penetration testing can be conducted internally or externally on the hardware, software, or firmware components of a system and can exercise both physical and technical controls. A standard method for penetration testing includes a pretest analysis based on full knowledge of the system, pretest identification of potential vulnerabilities based on the pretest analysis, and testing designed to determine the exploitability of vulnerabilities. All parties agree to the rules of engagement before commencing penetration testing scenarios. Organizations correlate the rules of engagement for the penetration tests with the tools, techniques, and procedures that are anticipated to be employed by adversaries. Penetration testing may result in the exposure of information that is protected by laws or regulations, to individuals conducting the testing. Rules of engagement, contracts, or other appropriate mechanisms can be used to communicate expectations for how to protect this information. Risk assessments guide the decisions on the level of independence required for the personnel conducting penetration testing.

Related Controls: [RA-5](#), [RA-10](#), [SA-11](#), [SR-5](#), [SR-6](#).

Control Enhancements:

(1) PENETRATION TESTING | [INDEPENDENT PENETRATION TESTING AGENT OR TEAM](#)

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

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

Related Controls: [CA-2](#).

(2) PENETRATION TESTING | [RED TEAM EXERCISES](#)

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

Discussion: Red team exercises extend the objectives of penetration testing by examining the security and privacy posture of organizations and the capability to implement effective cyber defenses. Red team exercises simulate attempts by adversaries to compromise mission and business functions and provide a comprehensive assessment of the security and

privacy posture of systems and organizations. Such attempts may include technology-based attacks and social engineering-based attacks. Technology-based attacks include interactions with hardware, software, or firmware components and/or mission and business processes. Social engineering-based attacks include interactions via email, telephone, shoulder surfing, or personal conversations. Red team exercises are most effective when conducted by penetration testing agents and teams with knowledge of and experience with current adversarial tactics, techniques, procedures, and tools. While penetration testing may be primarily laboratory-based testing, organizations can use red team exercises to provide more comprehensive assessments that reflect real-world conditions. The results from red team exercises can be used by organizations to improve security and privacy awareness and training and to assess control effectiveness.

Related Controls: None.

(3) PENETRATION TESTING | [FACILITY PENETRATION TESTING](#)

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

Discussion: Penetration testing of physical access points can provide information on critical vulnerabilities in the operating environments of organizational systems. Such information can be used to correct weaknesses or deficiencies in physical controls that are necessary to protect organizational systems.

Related Controls: [CA-2](#), [PE-3](#).

References: None.

[CA-9](#) INTERNAL SYSTEM CONNECTIONS

Control:

- a. Authorize internal connections of [Assignment: organization-defined system components or classes of components] to the system;
- b. Document, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated;
- c. Terminate internal system connections after [Assignment: organization-defined conditions]; and
- d. Review [Assignment: organization-defined frequency] the continued need for each internal connection.

Discussion: Internal system connections are connections between organizational systems and separate constituent system components (i.e., connections between components that are part of the same system) including components used for system development. Intra-system connections include connections with mobile devices, notebook and desktop computers, tablets, printers, copiers, facsimile machines, scanners, sensors, and servers. Instead of authorizing each internal system connection individually, organizations can authorize internal connections for a class of system components with common characteristics and/or configurations, including printers, scanners, and copiers with a specified processing, transmission, and storage capability or smart phones and tablets with a specific baseline configuration. The continued need for an internal system connection is reviewed from the perspective of whether it provides support for organizational missions or business functions.

Related Controls: [AC-3](#), [AC-4](#), [AC-18](#), [AC-19](#), [CM-2](#), [IA-3](#), [SC-7](#), [SI-12](#).

Control Enhancements:

(1) INTERNAL SYSTEM CONNECTIONS | [COMPLIANCE CHECKS](#)

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

Discussion: Compliance checks include verification of the relevant baseline configuration.

Related Controls: [CM-6](#).

References: [\[SP 800-124\]](#), [\[IR 8023\]](#).