## FISMA

NOTE: The format of the FISMA portion of this **TECH LOCK**® Certified Report is designed to be identical to the format of the Security Assessment Report (“SAR”) that the U.S. Department of Education requires its subcontractors to use.

The RESULTS column contains either an “S” (for a Satisfactory rating), or an “OS” (for an Other than Satisfactory rating). A rating of “S” indicates that the control is In Place. A rating of “OS” indicates that there are one or more findings or non-conformities for the control.

### Access Control (AC)

|  |  |  |
| --- | --- | --- |
| **AC-1** | **ACCESS CONTROL POLICY AND PROCEDURES** | **RESULTS** |
| **AC-1.1** | Determine if: |  |
| **AC-1.1.1** | 1. the organization develops and formally documents access control policy; |  |
| **AC-1.1.2** | 1. the organization access control policy addresses:  * purpose; * scope; * roles and responsibilities; * management commitment; * coordination among organizational entities; and * compliance; |  |
| **AC-1.1.3** | 1. the organization disseminates formal documented access control policy to elements within the organization having associated access control roles and responsibilities; |  |
| **AC-1.1.4** | 1. the organization develops and formally documents access control procedures; |  |
| **AC-1.1.5** | 1. the organization access control procedures facilitate implementation of the access control policy and associated access control controls; and |  |
| **AC-1.1.6** | 1. the organization disseminates formal documented access control procedures to elements within the organization having associated access control roles and responsibilities. |  |
| **AC-1.2** | Determine if: |  |
| **AC-1.2.1** | 1. the organization defines the frequency of access control policy reviews/updates; |  |
| **AC-1.2.2** | 1. the organization reviews/updates access control policy in accordance with organization-defined frequency; and |  |
| **AC-1.2.3** | 1. the organization defines the frequency of access control procedure reviews/updates; |  |
| **AC-1.2.4** | 1. the organization reviews/updates access control procedures in accordance with organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **AC-2** | **ACCOUNT MANAGEMENT** | **RESULTS** |
| **AC-2.1** | Determine if: |  |
| **AC-2.1.1** | 1. the organization manages information system accounts, including;  * identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary); * establishing conditions for group membership; * identifying authorized users of the information system and specifying access privileges; * requiring appropriate approvals for requests to establish accounts; * establishing, activating, modifying, disabling, and removing accounts; * specifically authorizing and monitoring the use of guest/anonymous and temporary accounts; * notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes; * deactivating: i) temporary accounts that are no longer required; and ii) accounts of terminated or transferred users; and * granting access to the system based on: * a valid access authorization; * intended system usage; and * other attributes as required by the organization or associated missions/business functions; and |  |
| **AC-2.1.2** | 1. the organization defines the frequency of information system account reviews; and |  |
| **AC-2.1.3** | 1. the organization reviews information system accounts in accordance with organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **AC-2(1)** | **ACCOUNT MANAGEMENT – CONTROL ENHANCEMENT** | **RESULTS** |
| **AC-2(1).1** | Determine if the organization employs automated mechanisms to support information system account management functions. |  |

|  |  |  |
| --- | --- | --- |
| **AC-2(2)** | **ACCOUNT MANAGEMENT – CONTROL ENHANCEMENT** | **RESULTS** |
| **AC-2(2).1** | Determine if: |  |
| **AC-2(2).1.1** | 1. the organization defines in the security plan, explicitly or by reference, a time period for each type of account after which the information system terminates temporary and emergency accounts; and |  |
| **AC-2(2).2.1** | 1. the information system automatically terminates temporary and emergency accounts after the organization-defined time period for each type of account. |  |

|  |  |  |
| --- | --- | --- |
| **AC-2(3)** | **ACCOUNT MANAGEMENT – CONTROL ENHANCEMENT** | **RESULTS** |
| **AC-2(3).1** | Determine if: |  |
| **AC-2(3).1.1** | 1. the organization defines in the security plan, explicitly or by reference, a time period after which the information system disables inactive accounts; and |  |
| **AC-2(3).2.1** | 1. the information system automatically disables inactive accounts after organization-defined time period. |  |

|  |  |  |
| --- | --- | --- |
| **AC-2(4)** | **ACCOUNT MANAGEMENT – CONTROL ENHANCEMENT** | **RESULTS** |
| **AC-2(4).1** | Determine if: |  |
| **AC-2(4).1.1** | 1. the information system automatically audits:  * account creation; * modification; * disabling; and * termination actions; and |  |
| **AC-2(4).1.2** | 1. the information system notifies, as required, appropriate individuals. |  |

|  |  |  |
| --- | --- | --- |
| **AC-3** | **ACCESS ENFORCEMENT** | **RESULTS** |
| **AC-3.1** | Determine if the information system enforces approved authorizations for logical access  to the system in accordance with applicable policy. |  |

|  |  |  |
| --- | --- | --- |
| **AC-4** | **INFORMATION FLOW ENFORCEMENT** | **RESULTS** |
| **AC-4.1** | Determine if: |  |
| **AC-4.1.1** | 1. The information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy; |  |

|  |  |  |
| --- | --- | --- |
| **AC-5** | **SEPARATION OF DUTIES** | **RESULTS** |
| **AC-5.1** | Determine if: |  |
| **AC-5.1.1** | 1. the organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals; and |  |
| **AC-5.1.2** | 1. the information system enforces separation of duties through assigned access authorizations. |  |

|  |  |  |
| --- | --- | --- |
| **AC-6** | **LEAST PRIVILEGE** | **RESULTS** |
| **AC-6.1** | Determine if: |  |
| **AC-6.1.1** | 1. the organization assigns the most restrictive set of rights/privileges or accesses needed by the users for the performance of specified tasks; and |  |
| **AC-6.1.2** | 1. the information system enforces the most restrictive set of rights/privileges or accesses needed by users. |  |

|  |  |  |
| --- | --- | --- |
| **AC-6(1)** | **LEAST PRIVILEGE – CONTROL ENHANCEMENT** | **RESULTS** |
| **AC-6(1).1** | Determine if: |  |
| **AC-6(1).1.1** | 1. the organization defines the security functions (deployed in hardware, software, and   firmware) and security-relevant information for which access must be explicitly  authorized; and |  |
| **AC-6(1).1.2** | 1. the organization explicitly authorizes access to the organization-defined security   functions and security-relevant information. |  |

|  |  |  |
| --- | --- | --- |
| **AC-6(2)** | **LEAST PRIVILEGE – CONTROL ENHANCEMENT** | **RESULTS** |
| **AC-6(2).1** | Determine if: |  |
| **AC-6(2).1.1** | 1. the organization defines the security functions or security-relevant information to   which users of information system accounts, or roles, have access; and |  |
| **AC-6(2).1.2** | 1. the organization requires that users of information system accounts, or roles, with   access to organization-defined security functions or security-relevant information,  use non-privileged accounts, or roles, when accessing other system functions; and |  |
| **AC-6(2).1.3** | 1. the organization, if deemed feasible, audits any use of privileged accounts, or roles,   with access to organization-defined security functions or security-relevant  information, when accessing other system functions. |  |

|  |  |  |
| --- | --- | --- |
| **AC-7** | **UNSUCCESSFUL LOGIN ATTEMPTS** | **RESULTS** |
| **AC-7.1** | Determine if: |  |
| **AC-7.1.1** | 1. the organization defines in the security plan, explicitly or by reference, the maximum number of consecutive invalid access attempts to the information system by a user and the time period in which the consecutive invalid access attempts occur; |  |
| **AC-7.1.2** | 1. the information system enforces the organization-defined limit of consecutive invalid access attempts by a user during the organization-defined time period; |  |
| **AC-7.1.3** | 1. the organization defines in the security plan, explicitly or by reference, the time period for lock out mode or delay period; |  |
| **AC-7.1.4** | 1. the organization selects either a lock out mode for the organization-defined time period or delays next login prompt for the organization-defined delay period for information system responses to consecutive invalid access attempts; and |  |
| **AC-7.1.5** | 1. the information system enforces the organization-selected lock out mode or delayed login prompt. |  |

|  |  |  |
| --- | --- | --- |
| **AC-8** | **SYSTEM USE NOTIFICATION** | **RESULTS** |
| **AC-8.1** | Determine if: |  |
| **AC-8.1.1** | 1. the information system displays a system use notification message before granting system access informing potential users:  * that the user is accessing a U.S. Government information system; * that the system usage may be monitored, recorded and subject to audit; * that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and * that the use of the system indicates consent to monitoring and recording; |  |
| **AC-8.1.2** | 1. the system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries); |  |
| **AC-8.1.3** | 1. the organization approves the information system use notification message before its use; and |  |
| **AC-8.1.4** | 1. the system use notification message remains on the screen until the users take explicit action to log on to the information system. |  |

|  |  |  |
| --- | --- | --- |
| **AC-11** | **SESSION LOCK** | **RESULTS** |
| **AC-11.1** | Determine if: |  |
| **AC-11.1.1** | 1. the organization defines in the security plan, explicitly or by reference, the time period of user inactivity after which the information system initiates a session lock; |  |
| **AC-11.1.2** | 1. the information system initiates a session lock after the organization-defined time period of inactivity; |  |
| **AC-11.1.3** | 1. the information system provides the capability for users to directly initiate session lock mechanisms; and |  |
| **AC-11.1.4** | 1. the information system maintains the session lock until the user reestablishes access using the appropriate identification and authentication procedures. |  |

|  |  |  |
| --- | --- | --- |
| **AC-14** | **PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION** | **RESULTS** |
| **AC-14.1** | Determine if: |  |
| **AC-14.1.1** | 1. the organization identifies and documents specific user actions that can be performed on the information system without identification or authentication. |  |

|  |  |  |
| --- | --- | --- |
| **AC-14(1)** | **PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION** | **RESULTS** |
| **AC-14(1).1** | Determine if: |  |
| **AC-14(1).1.1** | 1. the organization permits action to be performed without identification and authentication only to the extent necessary to accomplish mission objectives. |  |

|  |  |  |
| --- | --- | --- |
| **AC-17** | **REMOTE ACCESS** | **RESULTS** |
| **AC-17.1** | Determine if: |  |
| **AC-17.1.1** | 1. the organization authorizes, monitors, and controls remote access to the information system for all allowed methods of remote access to include both establishment of the remote connection and subsequent user actions across that connection. |  |

|  |  |  |
| --- | --- | --- |
| **AC-17(1)** | **REMOTE ACCESS – CONTROL ENHANCEMENT** | **RESULTS** |
| **AC-17(1).1** | Determine if: |  |
| **AC-17(1).1.1** | 1. The information system employs automated mechanisms to facilitate the monitoring and control of remote access methods. |  |

|  |  |  |
| --- | --- | --- |
| **AC-17(2)** | **REMOTE ACCESS – CONTROL ENHANCEMENT** | **RESULTS** |
| **AC-17(2).1** | Determine if: |  |
| **AC-17(2).1.1** | 1. the information system employs cryptography to protect the confidentiality and integrity of remote access sessions. |  |

|  |  |  |
| --- | --- | --- |
| **AC-17(3)** | **REMOTE ACCESS – CONTROL ENHANCEMENT** | **RESULTS** |
| **AC-17(3).1** | Determine if: |  |
| **AC-17(3).1.1** | 1. the organization defines managed access control points for remote access to the information system; and |  |
| **AC-17(3).2.1** | 1. the information system controls all remote access through a limited number of managed access control points. |  |

|  |  |  |
| --- | --- | --- |
| **AC-17(4)** | **REMOTE ACCESS – CONTROL ENHANCEMENT** | **RESULTS** |
| **AC-17(4).1** | Determine if: |  |
| **AC-17(4).1.1** | 1. the organization defines the situations and compelling operational needs when remote access to privileged functions on the information system is allowed; and |  |
| **AC-17(4).2.1** | 1. the organization permits remote access for privileged functions only for compelling operational needs and documents the rationale for such access in the security plan for the information system. |  |

|  |  |  |
| --- | --- | --- |
| **AC-17(5)** | **REMOTE ACCESS – CONTROL ENHANCEMENT** | **RESULTS** |
| **AC-17(5).1** | Determine if: |  |
| **AC-17(5).1.1** | 1. The organization monitors for unauthorized remote connections to the information system [Assignment: organization-defined frequency], and takes appropriate action if an unauthorized connection is discovered. |  |

|  |  |  |
| --- | --- | --- |
| **AC-17(7)** | **REMOTE ACCESS – CONTROL ENHANCEMENT** | **RESULTS** |
| **AC-17(7).1** | Determine if: |  |
| **AC-17(7).1.1** | 1. The organization ensures that remote sessions for accessing [Assignment: organization-defined list of security functions and security-relevant information] employ [Assignment: organization defined additional security measures] and are audited. |  |

|  |  |  |
| --- | --- | --- |
| **AC-17(8)** | **REMOTE ACCESS – CONTROL ENHANCEMENT** | **RESULTS** |
| **AC-17(8).1** | Determine if: |  |
| **AC-17(8).1.1** | 1. The organization disables all unnecessary ports and protocols except for explicitly identified components in support of specific operational requirements. |  |

|  |  |  |
| --- | --- | --- |
| **AC-18** | **WIRELESS ACCESS** | **RESULTS** |
| **AC-18.1** | Determine if: |  |
| **AC-18.1.1** | 1. the organization establishes usage restrictions and implementation guidance for wireless technologies; |  |
| **AC-18.1.2** | 1. the organization authorizes, monitors, and controls wireless access to the information system; and |  |
| **AC-18.1.3** | 1. the wireless access restrictions are consistent with NIST Special Publications 800-48 and 800-97 |  |

|  |  |  |
| --- | --- | --- |
| **AC-18(1)** | **WIRELESS ACCESS – CONTROL ENHANCEMENT** | **RESULTS** |
| **AC-18(1).1** | Determine if: |  |
| **AC-18(1).1.1** | 1. the organization uses authentication and encryption to protect wireless access to the information system. |  |

|  |  |  |
| --- | --- | --- |
| **AC-19** | **ACCESS CONTROL FOR MOBILE DEVICES** | **RESULTS** |
| **AC-19.1** | Determine if: |  |
| **AC-19.1.1** | 1. the organization establishes usage restrictions and implementation guidance for organization-controlled portable and mobile devices; and |  |
| **AC-19.1.2** | 1. the organization authorizes, monitors, and controls device access to organizational information systems. |  |

|  |  |  |
| --- | --- | --- |
| **AC-19(1)** | **ACCESS CONTROL FOR MOBILE DEVICES – CONTROL ENHANCEMENT** | **RESULTS** |
| **AC-19(1).1** | Determine if: |  |
| **AC-19(1).1.1** | 1. The organization restricts the use of writable, removable media in organizational information systems. |  |

|  |  |  |
| --- | --- | --- |
| **AC-19(2)** | **ACCESS CONTROL FOR MOBILE DEVICES – CONTROL ENHANCEMENT** | **RESULTS** |
| **AC-19(2).1** | Determine if: |  |
| **AC-19(2).1.1** | 1. The organization prohibits the use of personally owned, removable media in organizational information systems. |  |

|  |  |  |
| --- | --- | --- |
| **AC-19(3)** | **ACCESS CONTROL FOR MOBILE DEVICES – CONTROL ENHANCEMENT** | **RESULTS** |
| **AC-19(3).1** | Determine if: |  |
| **AC-19(3).1.1** | 1. The organization prohibits the use of removable media in organizational information systems when the media has no identifiable owner. |  |

|  |  |  |
| --- | --- | --- |
| **AC-20** | **USE OF EXTERNAL INFORMATION SYSTEMS** | **RESULTS** |
| **AC-20.1** | Determine if: |  |
| **AC-20.1.1** | 1. the organization establishes terms and conditions for authorized individuals to access the information system from an external system that include the types of applications that can be accessed on the organizational information system from the external information system and the maximum FIPS 199 security category of information that can be processed, stored, and transmitted on the external information system. |  |

|  |  |  |
| --- | --- | --- |
| **AC-20(1)** | **USE OF EXTERNAL INFORMATION SYSTEMS – CONTROL ENHANCEMENT** | **RESULTS** |
| **AC-20(1).1** | Determine if: |  |
| **AC-20(1).1.1** | 1. the organization prohibits authorized individuals from using an external information system to access the information system or to process, store, or transmit organization-controlled information except in situations where the organization:  * verifies, for authorized exceptions, the employment of required security controls on the external system as specified in the organization’s information security policy and system security plan when allowing connections to the external information system; or * approves, for authorized exceptions, information system connection or processing agreements with the organizational entity hosting the external information system. |  |

|  |  |  |
| --- | --- | --- |
| **AC-20(2)** | **USE OF EXTERNAL INFORMATION SYSTEMS – CONTROL ENHANCEMENT** | **RESULTS** |
| **AC-20(2).1** | Determine if the organization limits the use of organization-controlled portable storage  media by authorized individuals on external information systems. |  |

|  |  |  |
| --- | --- | --- |
| **AC-22** | **PUBLICLY ACCESSIBLE CONTENT** | **RESULTS** |
| **AC-22.1** | Determine if: |  |
| **AC-22.1.1** | 1. the organization designates individuals authorized to post information onto an organizational information system that is publicly accessible; |  |
| **AC-22.1.2** | 1. the organization trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information; |  |
| **AC-22.1.3** | 1. the organization reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto the organizational information system; |  |
| **AC-22.1.4** | 1. the organization defines the frequency of reviews of the content on the publicly accessible organizational information system for nonpublic information; |  |
| **AC-22.1.5** | 1. the organization reviews the content on the publicly accessible organizational information system for nonpublic information in accordance with the organization defined frequency; and |  |
| **AC-22.1.6** | 1. the organization removes nonpublic information from the publicly accessible organizational information system, if discovered. |  |

### Security Awareness and Training (AT)

|  |  |  |
| --- | --- | --- |
| **AT-1** | **SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES** | **RESULTS** |
| **AT-1.1** | Determine if: |  |
| **AT-1.1.1** | 1. the organization develops and formally documents awareness and training policy; |  |
| **AT-1.1.2** | 1. the organization awareness and training policy addresses:  * purpose; * scope; * roles and responsibilities; * management commitment; * coordination among organizational entities; and * compliance; |  |
| **AT-1.1.3** | 1. the organization disseminates formal documented awareness and training policy to elements within the organization having associated awareness and training roles and responsibilities; |  |
| **AT-1.1.4** | 1. the organization develops and formally documents awareness and training procedures; |  |
| **AT-1.1.5** | 1. the organization awareness and training procedures facilitate implementation of the awareness and training policy and associated awareness and training controls; and |  |
| **AT-1.1.6** | 1. the organization disseminates formal documented awareness and training procedures to elements within the organization having associated awareness and training roles and responsibilities. |  |
| **AT-1.2** | Determine if: |  |
| **AT-1.2.1** | 1. the organization defines the frequency of awareness and training policy reviews/updates; |  |
| **AT-1.2.2** | 1. the organization reviews/updates awareness and training policy in accordance with organization-defined frequency; and |  |
| **AT-1.2.3** | 1. the organization defines the frequency of awareness and training procedure reviews/updates; |  |
| **AT-1.2.4** | 1. the organization reviews/updates awareness and training procedures in accordance with organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **AT-2** | **SECURITY AWARENESS** | **RESULTS** |
| **AT-2.1** | Determine if: |  |
| **AT-2.1.1** | 1. the organization provides basic security awareness training to all information system users (including managers and senior executives) before authorizing access to the system and when required by system changes; |  |
| **AT-2.1.2** | 1. the security awareness training is consistent with applicable regulations and NIST Special Publication 800-50; |  |
| **AT-2.1.3** | 1. the security awareness and training materials address the specific requirements of the organization and the information systems to which personnel have authorized access; |  |
| **AT-2.1.4** | 1. the organization defines in the security plan, explicitly or by reference, the frequency of refresher security awareness training and the frequency is at least annually; and |  |
| **AT-2.1.5** | 1. the organization provides refresher security awareness training in accordance with organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **AT-3** | **SECURITY TRAINING** | **RESULTS** |
| **AT-3.1** | Determine if: |  |
| **AT-3.1.1** | 1. the organization identifies personnel with significant information system security responsibilities and roles and documents those roles and responsibilities; |  |
| **AT-3.1.2** | 1. the organization provides security training to personnel with identified information system security roles and responsibilities before authorizing access to the system or performing assigned duties when required by system changes; |  |
| **AT-3.1.3** | 1. the security training materials address the procedures and activities necessary to fulfill the organization-defined roles and responsibilities for information system security; |  |
| **AT-3.1.4** | 1. the security training is consistent with applicable regulations and NIST Special Publication 800-50; |  |
| **AT-3.1.5** | 1. the organization defines in the security plan, explicitly or by reference, the frequency of refresher security training; and |  |
| **AT-3.1.6** | 1. the organization provides refresher security training in accordance with organization-defined frequency, at least annually. |  |

|  |  |  |
| --- | --- | --- |
| **AT-4** | **SECURITY TRAINING RECORDS** | **RESULTS** |
| **AC-4.1** | Determine if: |  |
| **AT-4.1.1** | 1. the organization monitors and documents basic security awareness training and specific information system security training. |  |

### Audit and Accountability (AU)

|  |  |  |
| --- | --- | --- |
| **AU-1** | **AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES** | **RESULTS** |
| **AU-1.1** | Determine if: |  |
| **AU-1.1.1** | 1. the organization develops and formally documents audit and accountability policy; |  |
| **AU-1.1.2** | 1. the organization audit and accountability policy addresses:  * purpose; * scope; * roles and responsibilities; * management commitment; * coordination among organizational entities; and * compliance; |  |
| **AU-1.1.3** | 1. the organization disseminates formal documented audit and accountability policy to elements within the organization having associated audit and accountability roles and responsibilities; |  |
| **AU-1.1.4** | 1. the organization develops and formally documents audit and accountability procedures; |  |
| **AU-1.1.5** | 1. the organization audit and accountability procedures facilitate implementation of the audit and accountability policy and associated audit and accountability controls; and |  |
| **AU-1.1.6** | 1. the organization disseminates formal documented audit and accountability procedures to elements within the organization having associated audit and accountability roles and responsibilities. |  |
| **AU-1.2** | Determine if: |  |
| **AU-1.2.1** | 1. the organization defines the frequency of audit and accountability policy reviews/updates; |  |
| **AU-1.2.2** | 1. the organization reviews/updates audit and accountability policy in accordance with organization-defined frequency; and |  |
| **AU-1.2.3** | 1. the organization defines the frequency of audit and accountability procedure reviews/updates; |  |
| **AU-1.2.4** | 1. the organization reviews/updates audit and accountability procedures in accordance with organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **AU-2** | **AUDITABLE EVENTS** | **RESULTS** |
| **AU-2.1** | Determine if: |  |
| **AU-2.1.1** | 1. the organization defines in the security plan, explicitly or by reference, information system auditable events; |  |
| **AU-2.1.2** | 1. the organization-defined auditable events include those deemed by the organization to be adequate to support after-the-fact investigations of security incidents; |  |
| **AU-2.1.3** | 1. the information system generates audit records for the organization-defined auditable events; |  |
| **AU-2.1.4** | 1. the organization specifies which information system components carry out auditing activities; and |  |
| **AU-2.1.5** | 1. the organization decides, based upon a risk assessment, which events require auditing on a continuous basis and which events require auditing in response to specific situations. |  |

|  |  |  |
| --- | --- | --- |
| **AU-2(3)** | **AUDITABLE EVENTS – CONTROL ENHANCEMENT** | **RESULTS** |
| **AU-2(3).1** | Determine if: |  |
| **AU-2(3).1.1** | 1. the organization periodically reviews and updates the list of organization-defined auditable events. |  |

|  |  |  |
| --- | --- | --- |
| **AU-2(4)** | **AUDITABLE EVENTS – CONTROL ENHANCEMENT** | **RESULTS** |
| **AU-2(4).1** | Determine if the organization includes execution of privileged functions in the list of events to be audited by the information system. |  |

|  |  |  |
| --- | --- | --- |
| **AU-3** | **CONTENT OF AUDIT RECORDS** | **RESULTS** |
| **AU-3.1** | Determine if: |  |
| **AU-3.1.1** | 1. the information system audit records capture sufficient information to establish what events occurred; |  |
| **AU-3.1.2** | 1. the information system audit records capture sufficient information to establish the sources of the events; and |  |
| **AU-3.1.3** | 1. the information system audit records capture sufficient information to establish the outcomes of the events. |  |

|  |  |  |
| --- | --- | --- |
| **AU-3(1)** | **CONTENT OF AUDIT RECORDS – CONTROL ENHANCEMENT** | **RESULTS** |
| **AU-3(1).1** | Determine if the information system provides the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject. |  |

|  |  |  |
| --- | --- | --- |
| **AU-4** | **AUDIT STORAGE CAPACITY** | **RESULTS** |
| **AU-4.1** | Determine if: |  |
| **AU-4.1.1** | 1. the organization allocates sufficient audit record storage capacity; and |  |
| **AU-4.2.1** | 1. the organization configures auditing to reduce the likelihood of audit record storage capacity being exceeded. |  |

|  |  |  |
| --- | --- | --- |
| **AU-5** | **RESPONSE TO AUDIT PROCESSING FAILURES** | **RESULTS** |
| **AU-5.1** | Determine if: |  |
| **AU-5.1.1** | 1. the organization defines in the security plan, explicitly or by reference, actions to be taken in the event of an audit processing failure; |  |
| **AU-5.1.2** | 1. the organization defines in the security plan, explicitly or by reference, personnel to be notified in case of an audit processing failure; and |  |
| **AU-5.1.3** | 1. the information system alerts appropriate organizational officials and takes any additional organization-defined actions in the event of an audit failure, to include audit storage capacity being reached or exceeded. |  |

|  |  |  |
| --- | --- | --- |
| **AU-6** | **AUDIT REVIEW, ANALYSIS, AND REPORTING** | **RESULTS** |
| **AU-6.1** | Determine if: |  |
| **AU-6.1.1** | 1. the organization regularly reviews/analyzes audit records for indications of inappropriate or unusual activity; |  |
| **AU-6.1.2** | 1. the organization investigates suspicious activity or suspected violations; |  |
| **AU-6.1.3** | 1. the organization report’s findings of inappropriate/unusual activities, suspicious behavior, or suspected violations to appropriate officials; and |  |
| **AU-6.1.4** | 1. the organization takes necessary actions in response to the reviews/analyses of audit records. |  |
| **AU-6.2.1** | 1. the organization increases the level of audit monitoring and analysis activity whenever there is increased risk to organizational operations and assets, or to individuals, based on information from law enforcement organizations, the intelligence community, or other credible sources. |  |

|  |  |  |
| --- | --- | --- |
| **AU-7** | **AUDIT REDUCTION AND REPORT GENERATION** | **RESULTS** |
| **AU-7.1** | Determine if the information system provides audit reduction and report generation tools that support after-the-fact investigations of security incidents without altering original audit records. |  |

|  |  |  |
| --- | --- | --- |
| **AU-7(1)** | **AUDIT REDUCTION AND REPORT GENERATION – CONTROL ENHANCEMENT** | **RESULTS** |
| **AU-7(1).1** | Determine if the information system provides the capability to automatically process audit records for events of interest based upon selectable, event criteria. |  |

|  |  |  |
| --- | --- | --- |
| **AU-8** | **TIME STAMPS** | **RESULTS** |
| **AU-8.1** | Determine if the information system provides time stamps in audit records. |  |

|  |  |  |
| --- | --- | --- |
| **AU-8(1)** | **TIME STAMPS – CONTROL ENHANCEMENT** | **RESULTS** |
| **AU-8(1).1** | Determine if: |  |
| **AU-8(1).1.1** | 1. the organization defines in the security plan, explicitly or by reference, the frequency of internal clock synchronization for the information system; and |  |
| **AU-8(1).2.1** | 1. the organization synchronizes internal information system clocks periodically in accordance with organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **AU-9** | **PROTECTION OF AUDIT INFORMATION** | **RESULTS** |
| **AU-9.1** | Determine if the information system protects audit information and audit tools from unauthorized access, modification, and deletion. |  |

|  |  |  |
| --- | --- | --- |
| **AU-11** | **AUDIT RECORD RETENTION** | **RESULTS** |
| **AU-11.1** | Determine if: |  |
| **AU-11.1.1** | 1. the organization defines the retention period for audit records generated by the information system; and |  |
| **AU-11.1.2** | 1. the organization retains information system audit records for the organization-defined time period to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements. |  |

|  |  |  |
| --- | --- | --- |
| **AU-12** | **AUDIT GENERATION** | **RESULTS** |
| **AU-12.1** | Determine if: |  |
| **AU-12.1.1** | 1. the organization defines the information system components that provide audit record generation capability for the list of auditable events defined in AU-2; |  |
| **AU-12.1.2** | 1. the information system provides audit record generation capability, at organization-defined information system components, for the list of auditable events defined in AU-2; |  |
| **AU-12.1.3** | 1. the information system allows designated organizational personnel to select which auditable events are to be audited by specific components of the system; and |  |
| **AU-12.1.4** | 1. the information system generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3. |  |

### Security Assessment and Authorization (CA)

|  |  |  |
| --- | --- | --- |
| **CA-1** | **SECURITY ASSESSMENTS AND AUTHORIZATION POLICIES AND PROCEDURES** | **RESULTS** |
| **CA-1.1** | Determine if: |  |
| **CA-1.1.1** | 1. the organization develops and formally documents security assessment and authorization policy; |  |
| **CA-1.1.2** | 1. the organization security assessment and authorization policy addresses:  * purpose; * scope; * roles and responsibilities; * management commitment; * coordination among organizational entities; and * compliance; |  |
| **CA-1.1.3** | 1. the organization disseminates formal documented security assessment and authorization policy to elements within the organization having associated security assessment and authorization roles and responsibilities; |  |
| **CA-1.1.4** | 1. the organization develops and formally documents security assessment and authorization procedures; |  |
| **CA-1.1.5** | 1. the organization security assessment and authorization procedures facilitate implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and |  |
| **CA-1.1.6** | 1. the organization disseminates formal documented security assessment and authorization procedures to elements within the organization having associated security assessment and authorization roles and responsibilities. |  |
| **CA-1.2** | Determine if: |  |
| **CA-1.2.1** | 1. the organization defines the frequency of security assessment and authorization policy reviews/updates; |  |
| **CA-1.2.2** | 1. the organization reviews/updates security assessment and authorization policy in accordance with organization-defined frequency; and |  |
| **CA-1.2.3** | 1. the organization defines the frequency of security assessment and authorization procedure reviews/updates; |  |
| **CA-1.2.4** | 1. the organization reviews/updates security assessment and authorization procedures in accordance with organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **CA-2** | **SECURITY ASSESSMENTS** | **RESULTS** |
| **CA-2.1** | Determine if: |  |
| **CA-2.1.1** | 1. the organization defines in the security plan, explicitly or by reference, the frequency of security control assessments and the frequency is at least annually; and |  |
| **CA-2.1.2** | 1. the organization conducts an assessment of the security controls in the information system at an organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **CA-2(1)** | **SECURITY ASSESSMENTS – CONTROL ENHANCEMENT** | **RESULTS** |
| **CA-2.1(1)** | Determine if the organization employs an independent assessor or assessment team to conduct an assessment of the security controls in the information system. |  |

|  |  |  |
| --- | --- | --- |
| **CA-3** | **INFORMATION SYSTEM CONNECTIONS** | **RESULTS** |
| **CA-3.1** | Determine if: |  |
| **CA-3.1.1** | 1. the organization identifies all connections to external information systems (i.e., information systems outside of the accreditation boundary); |  |
| **CA-3.1.2** | 1. the organization authorizes all connections from the information system to external information systems through the use of system connection agreements; and |  |
| **CA-3.1.3** | 1. the organization monitors/controls the system interconnections on an ongoing basis. |  |

|  |  |  |
| --- | --- | --- |
| **CA-5** | **PLAN OF ACTION AND MILESTONES** | **RESULTS** |
| **CA-5.1** | Determine if: |  |
| **CA-5.1.1** | 1. the organization develops a plan of action and milestones for the information system; |  |
| **CA-5.1.2** | 1. the plan of action and milestones documents the planned, implemented, and evaluated remedial actions by the organization to correct deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; |  |
| **CA-5.1.3** | 1. the organization defines in the security plan, explicitly or by reference, the frequency of plan of action and milestone updates; and |  |
| **CA-5.1.4** | 1. the organization updates the plan of action and milestones at an organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **CA-6** | **SECURITY AUTHORIZATION** | **RESULTS** |
| **CA-6.1** | Determine if: |  |
| **CA-6.1.1** | 1. the organization defines in the security plan, explicitly or by reference, the frequency of authorization updates, not to exceed three years; |  |
| **CA-6.1.2** | 1. the organization authorizes (i.e., accredits) the information system for processing before operations and updates the authorization at an organization-defined frequency or when there is a significant change to the information system; |  |
| **CA-6.1.3** | 1. a senior organizational official signs and approves the security accreditation; and |  |
| **CA-6.1.4** | 1. the security accreditation process employed by the organization is consistent with NIST Special Publications 800-37. |  |

|  |  |  |
| --- | --- | --- |
| **CA-7** | **CONTINUOUS MONITORING** | **RESULTS** |
| **CA-7.1** | Determine if: |  |
| **CA-7.1.1** | 1. the organization monitors the security controls in the information system on an ongoing basis; and |  |
| **CA-7.1.2** | 1. the organization employs a security control monitoring process consistent with NIST Special Publications 800-37 and 800-53A. |  |
| **CA-7.2.1** | 1. the organization conducts security impact analyses on changes to the information system; |  |
| **CA-7.2.2** | 1. the organization documents and reports changes to or deficiencies in the security controls employed in the information system; and |  |
| **CA-7.2.3** | 1. the organization makes adjustments to the information system security plan and plan of action and milestones, as appropriate, based on the activities associated with continuous monitoring of the security controls. |  |

### Configuration Management (CM)

|  |  |  |
| --- | --- | --- |
| **CM-1** | **CONFIGURATION MANAGEMENT POLICY AND PROCEDURES** | **RESULTS** |
| **CM-1.1** | Determine if: |  |
| **CM-1.1.1** | 1. the organization develops and formally documents configuration management policy; |  |
| **CM-1.1.2** | 1. the organization configuration management policy addresses:  * purpose; * scope; * roles and responsibilities; * management commitment; * coordination among organizational entities; and * compliance; |  |
| **CM-1.1.3** | 1. the organization disseminates formal documented configuration management policy to elements within the organization having associated configuration management roles and responsibilities; |  |
| **CM-1.1.4** | 1. the organization develops and formally documents configuration management procedures; |  |
| **CM-1.1.5** | 1. the organization configuration management procedures facilitate implementation of the configuration management policy and associated configuration management controls; and |  |
| **CM-1.1.6** | 1. the organization disseminates formal documented configuration management procedures to elements within the organization having associated configuration management roles and responsibilities. |  |
| **CM-1.2** | Determine if: |  |
| **CM-1.2.1** | 1. the organization defines the frequency of configuration management policy reviews/updates; |  |
| **CM-1.2.2** | 1. the organization reviews/updates configuration management policy in accordance with organization-defined frequency; and |  |
| **CM-1.2.3** | 1. the organization defines the frequency of configuration management procedure reviews/updates; |  |
| **CM-1.2.4** | 1. the organization reviews/updates configuration management procedures in accordance with organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **CM-2** | **BASELINE CONFIGURATION** | **RESULTS** |
| **CM-2.1** | Determine if: |  |
| **CM-2.1.1** | 1. the organization develops and documents a baseline configuration of the information system that is consistent with the Federal Enterprise Architecture, shows relationships among information system components, and provides a well-defined and documented specification to which the information system is built; |  |
| **CM-2.1.2** | 1. the organization maintains the baseline configuration; and |  |
| **CM-2.1.3** | 1. the organization documents deviations from the baseline configuration, in support of mission needs/objectives. |  |

|  |  |  |
| --- | --- | --- |
| **CM-2(1)** | **BASELINE CONFIGURATION – CONTROL ENHANCEMENT** | **RESULTS** |
| **CM-2(1).1** | Determine if the organization updates the baseline configuration of the information system as an integral part of information system component installations. |  |

|  |  |  |
| --- | --- | --- |
| **CM-2(3)** | **BASELINE CONFIGURATION – CONTROL ENHANCEMENT** | **RESULTS** |
| **CM-2(3).1** | Determine if the organization retains older versions of baseline configurations as deemed necessary to support rollback. |  |

|  |  |  |
| --- | --- | --- |
| **CM-2(4)** | **BASELINE CONFIGURATION – CONTROL ENHANCEMENT** | **RESULTS** |
| **CM-2(4).1** | Determine if: |  |
| **CM-2(4).1.1** | 1. the organization develops and maintains a list of software programs not authorized to execute on the information system; and |  |
| **CM-2(4).1.2** | 1. the organization employs an allow-all, deny-by-exception authorization policy to identify software allowed to execute on the information system. |  |

|  |  |  |
| --- | --- | --- |
| **CM-3** | **CONFIGURATION CHANGE CONTROL** | **RESULTS** |
| **CM-3.1** | Determine if: |  |
| **CM-3.1.1** | 1. the organization authorizes, documents, and controls changes to the information system using an organizationally approved process; |  |
| **CM-3.1.2** | 1. the organization configuration change control involves the systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the information system, including upgrades and modifications; |  |
| **CM-3.1.3** | 1. the organization approves changes to the information system with consideration for the results from the security impact analysis of the change; and |  |
| **CM-3.1.4** | 1. the organization audits activities associated with configuration changes to the information system. |  |

|  |  |  |
| --- | --- | --- |
| **CM-3(2)** | **CONFIGURATION CHANGE CONTROL – CONTROL ENHANCEMENT** | **RESULTS** |
| **CM-3(2).1** | Determine if the organization tests, validates, and documents changes to the information system before implementing the changes on the operational system. |  |

|  |  |  |
| --- | --- | --- |
| **CM-4** | **SECURITY IMPACT ANALYSIS** | **RESULTS** |
| **CM-4.1** | Determine if the organization monitors changes to the information system by verifying that the organization:   * prior to change implementation and as part of the change approval process, conducts security impact analyses to assess the effects of the system changes; * after the system is changed (including upgrades and modifications), checks the security features to confirm that the features are still functioning properly; and * audits activities associated with configuration changes to the information system. |  |

|  |  |  |
| --- | --- | --- |
| **CM-5** | **ACCESS RESTRICTIONS FOR CHANGE** | **RESULTS** |
| **CM-5.1** | Determine if: |  |
| **CM-5.1.1** | 1. the organization approves individual access privileges and enforces physical and logical access restrictions associated with changes to the information system, including upgrades, and modifications; and |  |
| **CM-5.1.2** | 1. the organization generates, retains, and reviews records reflecting all such changes to the information system. |  |

|  |  |  |
| --- | --- | --- |
| **CM-6** | **CONFIGURATION SETTINGS** | **RESULTS** |
| **CM-6.1** | Determine if: |  |
| **CM-6.1.1** | 1. the organization establishes mandatory configuration settings for information technology products employed within the information system; |  |
| **CM-6.1.2** | 1. the organization configures the security settings of information technology products to the most restrictive mode consistent with operational requirements; |  |
| **CM-6.1.3** | 1. the organization documents the configuration settings; |  |
| **CM-6.1.4** | 1. the organization enforces the configuration settings in all components of the information system; and |  |
| **CM-6.1.5** | 1. the organization monitors and controls changes to the configuration settings in accordance with organizational policies and procedures. |  |

|  |  |  |
| --- | --- | --- |
| **CM-6(3)** | **CONFIGURATION SETTINGS – CONTROL ENHANCEMENT** | **RESULTS** |
| **CM-6(3).1** | Determine if: |  |
| **CM-6(3).1.1** | 1. the organization incorporates detection of unauthorized, security-relevant configuration changes into the organization’s incident response capability; and |  |
| **CM-6(3).1.2** | 1. the organization ensures that such detected events are tracked, monitored, corrected, and available for historical purposes. |  |

|  |  |  |
| --- | --- | --- |
| **CM-7** | **LEAST FUNCTIONALITY** | **RESULTS** |
| **CM-7.1** | Determine if: |  |
| **CM-7.1.1** | 1. the organization defines in the security plan, explicitly or by reference, prohibited or restricted functions, ports, protocols, and services for the information system; |  |
| **CM-7.1.2** | 1. the organization configures the information system to provide only essential capabilities; and |  |
| **CM-7.1.3** | 1. the organization configures the information system to specifically prohibit and/or restrict the use of organization-defined functions, ports, protocols, and/or services. |  |

|  |  |  |
| --- | --- | --- |
| **CM-7(1)** | **LEAST FUNCTIONALITY – CONTROL ENHANCEMENT** | **RESULTS** |
| **CM-7(1).1** | Determine if: |  |
| **CM-7(1).1.1** | 1. the organization defines the frequency of information system reviews to identify and eliminate unnecessary: - functions; - ports; - protocols; and/or - services; and |  |
| **CM-7(1).1.2** | 1. the organization reviews the information system in accordance with organization-defined frequency to identify and eliminate unnecessary: - functions; - ports; - protocols; and/or - services. |  |

|  |  |  |
| --- | --- | --- |
| **CM-8** | **INFORMATION SYSTEM COMPONENT INVENTORY** | **RESULTS** |
| **CM-8.1** | Determine if: |  |
| **CM-8.1.1** | 1. the organization develops and documents an inventory of the components of the information system:  * that is at the level of granularity deemed appropriate by the organization for the components included in the inventory that are subject to tracking and reporting; * that includes any information determined to be necessary by the organization to achieve effective property accountability; and * that is consistent with the accreditation boundary of the system; and |  |
| **CM-8.1.2** | 1. the organization maintains the inventory of the components of the information system to reflect the current state of the system. |  |

|  |  |  |
| --- | --- | --- |
| **CM-8(1)** | **INFORMATION SYSTEM COMPONENT INVENTORY – CONTROL ENHANCEMENT** | **RESULTS** |
| **CM-8(1).1** | Determine if the organization verifies that all components within the authorization boundary of the information system are either inventoried as a part of the system or recognized by another system as a component within that system. |  |

|  |  |  |
| --- | --- | --- |
| **CM-8(5)** | **INFORMATION SYSTEM COMPONENT INVENTORY – CONTROL ENHANCEMENT** | **RESULTS** |
| **CM-8(5).1** | Determine if: |  |
| **CM-8(5).1.1** | 1. the organization updates the inventory of information system components as an integral part of component installations. |  |

|  |  |  |
| --- | --- | --- |
| **CM-9** | **CONFIGURATION MANAGEMENT PLAN** | **RESULTS** |
| **CM-9.1** | Determine if the organization develops, documents, and implements a configuration  management plan for the information system that:   * addresses roles, responsibilities, and configuration management processes and procedures; * defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management; and * establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items. |  |

### Contingency Planning (CP)

|  |  |  |
| --- | --- | --- |
| **CP-1** | **CONTINGENCY PLANNING POLICY AND PROCEDURES** | **RESULTS** |
| **CP-1.1** | Determine if: |  |
| **CP-1.1.1** | 1. the organization develops and formally documents contingency planning policy; |  |
| **CP-1.1.2** | 1. the organization contingency planning policy addresses:  * purpose; * scope; * roles and responsibilities; * management commitment; * coordination among organizational entities; and compliance; |  |
| **CP-1.1.3** | 1. the organization disseminates formal documented contingency planning policy to elements within the organization having associated contingency planning roles and responsibilities; |  |
| **CP-1.1.4** | 1. the organization develops and formally documents contingency planning procedures; |  |
| **CP-1.1.5** | 1. the organization contingency planning procedures facilitate implementation of the contingency planning policy and associated contingency planning controls; and |  |
| **CP-1.1.6** | 1. the organization disseminates formal documented contingency planning procedures to elements within the organization having associated contingency planning roles and responsibilities. |  |
| **CP-1.2** | Determine if: |  |
| **CP-1.2.1** | 1. the organization defines the frequency of contingency planning policy reviews/updates; |  |
| **CP-1.2.2** | 1. the organization reviews/updates contingency planning policy in accordance with organization-defined frequency; and |  |
| **CP-1.2.3** | 1. the organization defines the frequency of contingency planning procedure reviews/updates; |  |
| **CP-1.2.4** | 1. the organization reviews/updates contingency planning procedures in accordance with organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **CP-2** | **CONTINGENCY PLAN** | **RESULTS** |
| **CP-2.1** | Determine if: |  |
| **CP-2.1.1** | 1. the organization and documents a contingency plan for the information system; |  |
| **CP-2.1.2** | 1. the contingency plan is consistent with NIST Special Publication 800-34; and |  |
| **CP-2.1.3** | 1. the contingency plan addresses contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the information system after a disruption or failure; |  |
| **CP-2.1.4** | 1. the contingency plan is reviewed and approved by designated organizational officials; and |  |
| **CP-2.1.5** | 1. the organization disseminates the contingency plan to key contingency personnel. |  |

|  |  |  |
| --- | --- | --- |
| **CP-2(1)** | **CONTINGENCY PLAN – CONTROL ENHANCEMENT** | **RESULTS** |
| **CP-2(1).1** | Determine if the organization coordinates the contingency plan with other related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan, and Emergency Action Plan). |  |

|  |  |  |
| --- | --- | --- |
| **CP-3** | **CONTINGENCY TRAINING** | **RESULTS** |
| **CP-3.1** | Determine if: |  |
| **CP-3.1.1** | 1. the organization provides contingency training to personnel with contingency roles and responsibilities; |  |
| **CP-3.1.2** | 1. the organization defines in the security plan, explicitly or by reference, the frequency of refresher contingency training and the frequency is at least annually; and |  |
| **CP-3.1.3** | 1. the organization provides initial training and refresher training in accordance with organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **CP-4** | **CONTINGENCY PLAN TESTING AND EXERCISES** | **RESULTS** |
| **CP-4.1** | Determine if: |  |
| **CP-4.1.1** | 1. the organization defines in the security plan, explicitly or by reference, the contingency plan tests and/or exercises to be conducted; |  |
| **CP-4.1.2** | 1. the organization defines in the security plan, explicitly or by reference, the frequency of contingency plan tests and/or exercises and the frequency is at least annually; |  |
| **CP-4.1.3** | 1. the organization tests/exercises the contingency plan using organization-defined tests/exercises in accordance with organization-defined frequency; and |  |
| **CP-4.1.4** | 1. the organization reviews the contingency plan test/exercise results and takes corrective actions. |  |
| **CP-4.2.1** | 1. the contingency plan tests/exercises confirm the plan’s effectiveness; |  |
| **CP-4.2.2** | 1. the contingency plan tests/exercises confirm the organization’s readiness to execute the plan; and |  |
| **CP-4.2.3** | 1. the contingency plan tests/exercises confirm the effects on organizational operations and assets (e.g., reduction in mission capability) and individuals arising due to contingency operations in accordance with the plan. |  |

|  |  |  |
| --- | --- | --- |
| **CP-4(1)** | **CONTINGENCY PLAN TESTING AND EXERCISES – CONTROL ENHANCEMENT** | **RESULTS** |
| **CP-4(1).1** | Determine if the organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan, and Emergency Action Plan). |  |

|  |  |  |
| --- | --- | --- |
| **CP-6** | **ALTERNATE STORAGE SITE** | **RESULTS** |
| **CP-6.1** | Determine if: |  |
| **CP-6.1.1** | 1. the organization identifies an alternate storage site; and |  |
| **CP-6.1.2** | 1. the organization initiates necessary alternate storage site agreements to permit storage of information system backup information. |  |

|  |  |  |
| --- | --- | --- |
| **CP-6(1)** | **ALTERNATE STORAGE SITE – CONTROL ENHANCEMENT** | **RESULTS** |
| **CP-6(1).1** | Determine if: |  |
| **CP-6(1).1.1** | 1. the contingency plan or Contingency Planning Policy identifies the primary storage site hazards; and |  |
| **CP-6(1).1.2** | 1. the alternate storage site is sufficiently separated from the primary storage site so as not to be susceptible to the same hazards identified at the primary site. |  |

|  |  |  |
| --- | --- | --- |
| **CP-6(3)** | **ALTERNATE STORAGE SITE – CONTROL ENHANCEMENT** | **RESULTS** |
| **CP-6(3).1** | Determine if: |  |
| **CP-6(3).1.1** | 1. the organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster; and |  |
| **CP-6(3).1.2** | 1. the organization defines explicit mitigation actions for potential accessibility problems. |  |

|  |  |  |
| --- | --- | --- |
| **CP-7** | **ALTERNATE PROCESSING SITE** | **RESULTS** |
| **CP-7.1** | Determine if: |  |
| **CP-7.1.1** | 1. the organization identifies an alternate processing site; |  |
| **CP-7.1.2** | 1. the organization defines in the security plan, explicitly or by reference, the time period within which processing must be resumed at the alternate processing site; and |  |
| **CP-7.1.3** | 1. the organization initiates necessary alternate processing site agreements to permit the resumption of information system operations for critical mission/business functions within organization-defined time period. |  |

|  |  |  |
| --- | --- | --- |
| **CP-7(1)** | **ALTERNATE PROCESSING SITE – CONTROL ENHANCEMENT** | **RESULTS** |
| **CP-7(1).1** | Determine if: |  |
| **CP-7(1).1.1** | 1. the contingency plan identifies the primary processing site hazards; and |  |
| **CP-7(1).1.2** | 1. the alternate processing site is sufficiently separated from the primary processing site so as not to be susceptible to the same hazards identified at the primary site. |  |

|  |  |  |
| --- | --- | --- |
| **CP-7(2)** | **ALTERNATE PROCESSING SITE – CONTROL ENHANCEMENT** | **RESULTS** |
| **CP-7(2).1** | Determine if: |  |
| **CP-7(2).1.1** | 1. the contingency plan identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster; and |  |
| **CP-7(2).1.2** | 1. the contingency plan defines explicit mitigation actions for potential accessibility problems. |  |

|  |  |  |
| --- | --- | --- |
| **CP-7(3)** | **ALTERNATE PROCESSING SITE – CONTROL ENHANCEMENT** | **RESULTS** |
| **CP-7(3).1** | Determine if alternate processing site agreements contain priority-of-service provisions in accordance with the organization’s availability requirements. |  |

|  |  |  |
| --- | --- | --- |
| **CP-7(5)** | **ALTERNATE PROCESSING SITE – CONTROL ENHANCEMENT** | **RESULTS** |
| **CP-7(5).1** | Determine if the alternate processing site provides information security measures equivalent to that of the primary site. |  |

|  |  |  |
| --- | --- | --- |
| **CP-8** | **TELECOMMUNICATIONS SERVICES** | **RESULTS** |
| **CP-8.1** | Determine if: |  |
| **CP-8.1.1** | 1. the organization identifies primary and alternate telecommunications services to support the information system; |  |
| **CP-8.1.2** | 1. the organization defines in the security plan, explicitly or by reference, the time period within which resumption of information system operations must take place; and |  |
| **CP-8.1.3** | 1. the organization initiates necessary alternate telecommunications service agreements to permit the resumption of telecommunications services for critical mission/business functions within the organization-defined time period when the primary telecommunications capabilities are unavailable. |  |
| **CP-8.2.1** | 1. the organization requests Telecommunications Service Priority (TSP) for all telecommunications services used for national security emergency preparedness when the primary and/or alternate telecommunications services are provided by a common carrier. |  |

|  |  |  |
| --- | --- | --- |
| **CP-8(1)** | **TELECOMMUNICATIONS SERVICES – CONTROL ENHANCEMENT** | **RESULTS** |
| **CP-8(1).1** | Determine if the organization develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with organizational availability requirements. |  |

|  |  |  |
| --- | --- | --- |
| **CP-8(2)** | **TELECOMMUNICATIONS SERVICES – CONTROL ENHANCEMENT** | **RESULTS** |
| **CP-8(2).1** | Determine if the organization obtains alternate telecommunications services that do not share a single point of failure with primary telecommunications services. |  |

|  |  |  |
| --- | --- | --- |
| **CP-9** | **INFORMATION SYSTEM BACKUP** | **RESULTS** |
| **CP-9.1** | Determine if: |  |
| **CP-9.1.1** | 1. the organization defines the frequency of information systems backups; |  |
| **CP-9.1.2** | 1. the organization backs up user-level and system-level information (including system state information) in accordance with the organization-defined frequency; and |  |
| **CP-9.1.3** | 1. the organization backs up information to alternate storage sites (if so designated) at a frequency and transfer rate consistent with the organization’s recovery time objectives and recovery point objectives. |  |
| **CP-9.2.1** | 1. the organization protects backup information at the designated storage locations. |  |

|  |  |  |
| --- | --- | --- |
| **CP-9(1)** | **INFORMATION SYSTEM BACKUP – CONTROL ENHANCEMENT** | **RESULTS** |
| **CP-9(1).1** | Determine if: |  |
| **CP-9(1).1.1** | 1. the organization defines in the security plan, explicitly or by reference, the frequency of information system backup testing; |  |
| **CP-9(1).1.2** | 1. the organization conducts information system backup testing in accordance with organization-defined frequency; and |  |
| **CP-9(1).1.3** | 1. testing results verify backup media reliability and information integrity. |  |

|  |  |  |
| --- | --- | --- |
| **CP-10** | **INFORMATION SYSTEM RECOVERY AND RECONSTITUTION** | **RESULTS** |
| **CP-10.1** | Determine if the organization provides and applies mechanisms and procedures for recovery and reconstitution of the information system to known secure state after disruption or failure. |  |

|  |  |  |
| --- | --- | --- |
| **CP-10(2)** | **INFORMATION SYSTEM RECOVERY AND RECONSTITUTION – CONTROL ENHANCEMENT** | **RESULTS** |
| **CP-10(2).1** | Determine if the information system implements transaction recovery for systems that are transaction-based. |  |

|  |  |  |
| --- | --- | --- |
| **CP-10(3)** | **INFORMATION SYSTEM RECOVERY AND RECONSTITUTION – CONTROL ENHANCEMENT** | **RESULTS** |
| **CP-10(3).1** | Determine if: |  |
| **CP-10(3).1.1** | 1. the organization defines in the security plan, explicitly or by reference, the circumstances that can inhibit recovery and reconstitution of the information system to a known state; and |  |
| **CP-10(3).1.2** | 1. the organization provides compensating security controls for organization-defined circumstances that can inhibit recovery and reconstitution of the information system to a known state. |  |

### Identification and Authentication (IA)

|  |  |  |
| --- | --- | --- |
| **IA-1** | **IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES** | **RESULTS** |
| **IA-1.1** | Determine if: |  |
| **IA-1.1.1** | 1. the organization develops and formally documents identification and authentication policy; |  |
| **IA-1.1.2** | 1. the organization identification and authentication policy addresses:  * purpose; * scope; * roles and responsibilities; * management commitment; * coordination among organizational entities; and * compliance; |  |
| **IA-1.1.3** | 1. the organization disseminates formal documented identification and authentication policy to elements within the organization having associated identification and authentication roles and responsibilities; |  |
| **IA-1.1.4** | 1. the organization develops and formally documents identification and authentication procedures; |  |
| **IA-1.1.5** | 1. the organization identification and authentication procedures facilitate implementation of the identification and authentication policy and associated identification and authentication controls; and |  |
| **IA-1.1.6** | 1. the organization disseminates formal documented identification and authentication procedures to elements within the organization having associated identification and authentication roles and responsibilities. |  |
| **IA-1.2** | Determine if: |  |
| **IA-1.2.1** | 1. the organization defines the frequency of identification and authentication policy reviews/updates; |  |
| **IA-1.2.2** | 1. the organization reviews/updates identification and authentication policy in accordance with organization-defined frequency; and |  |
| **IA-1.2.3** | 1. the organization defines the frequency of identification and authentication procedure reviews/updates; |  |
| **IA-1.2.4** | 1. the organization reviews/updates identification and authentication procedures in accordance with organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **IA-2** | **USER IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)** | **RESULTS** |
| **IA-2.1** | Determine if: |  |
| **IA-2.1.1** | 1. The information system uniquely identifies and authenticates users (or processes acting on behalf of users); and |  |
| **IA-2.1.2** | 1. Authentication levels for users (or processes acting on behalf of users) are consistent with NIST Special Publication 800-63 and e-authentication risk assessment results. |  |

|  |  |  |
| --- | --- | --- |
| **IA-2(1)** | **USER IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) – CONTROL ENHANCEMENT** | **RESULTS** |
| **IA-2(1).1** | Determine if: |  |
| **IA-2(1).1.1** | 1. the organization defines in the security plan, explicitly or by reference, the NIST Special Publication 800-63 authentication levels for the information system; and |  |
| **IA-2(1).1.2** | 1. the information system employs multifactor authentication for remote system access that is NIST Special Publication 800-63 compliant in accordance with the organizational selection of level 3, level 3 using a hardware authentication device or level 4. |  |

|  |  |  |
| --- | --- | --- |
| **IA-2(2)** | **USER IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) – CONTROL ENHANCEMENT** | **RESULTS** |
| **IA-2(2).1** | Determine if the information system uses multifactor authentication for network access to non-privileged accounts. |  |

|  |  |  |
| --- | --- | --- |
| **IA-2(3)** | **USER IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) – CONTROL ENHANCEMENT** | **RESULTS** |
| **IA-2(3).1** | Determine if the information system uses multifactor authentication for local access to privileged accounts. |  |

|  |  |  |
| --- | --- | --- |
| **IA-2(8)** | **USER IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) – CONTROL ENHANCEMENT** | **RESULTS** |
| **IA-2(8).1** | Determine if: |  |
| **IA-2(8).1.1** | 1. the organization defines the replay-resistant authentication mechanisms to be used for network access to privileged accounts; and |  |
| **IA-2(8).1.2** | 1. the information system uses the organization-defined replay-resistant authentication mechanisms for network access to privileged accounts. |  |

|  |  |  |
| --- | --- | --- |
| **IA-3** | **DEVICE IDENTIFICATION AND AUTHENTICATION** | **RESULTS** |
| **IA-3.1** | Determine if: |  |
| **IA-3.1.1** | 1. the organization defines the devices for which identification and authentication is required before establishing connections to the information system; |  |
| **IA-3.1.2** | 1. the information system uniquely identifies and authenticates the devices defined by the organization before establishing connections to the information system; and |  |
| **IA-3.1.3** | 1. the information system employs device authentication mechanisms with strength of mechanism determined by the FIPS 199 security categorization of the information system. |  |

|  |  |  |
| --- | --- | --- |
| **IA-4** | **IDENTIFIER MANAGEMENT** | **RESULTS** |
| **IA-4.1** | Determine if: |  |
| **IA-4.1.1** | 1. the organization manages user identifiers by uniquely identifying each user; |  |
| **IA-4.1.2** | 1. the organization manages user identifiers by verifying the identity of each user; |  |
| **IA-4.1.3** | 1. the organization manages user identifiers by receiving authorization to issue a user identifier from an appropriate organization official; |  |
| **IA-4.1.4** | 1. the organization manages user identifiers by issuing the identifier to the intended party; |  |
| **IA-4.1.5** | 1. the organization defines in the security plan, explicitly or by reference, the time period of inactivity after which a user identifier is to be disabled; |  |
| **IA-4.1.6** | 1. the organization manages user identifiers by disabling the identifier after the organization-defined time period of inactivity; and |  |
| **IA-4.1.7** | 1. the organization manages user identifiers by archiving identifiers. |  |

|  |  |  |
| --- | --- | --- |
| **IA-5** | **AUTHENTICATOR MANAGEMENT** | **RESULTS** |
| **IA-5.1** | Determine if: |  |
| **IA-5.1.1** | 1. the organization defines the time period (by authenticator type) for changing/refreshing authenticators; and |  |
| **IA-5.1.2** | 1. the organization manages information system authenticators for users and devices by:  * verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator; * establishing initial authenticator content for authenticators defined by the organization; * ensuring that authenticators have sufficient strength of mechanism for their intended use; * establishing and implementing administrative procedures for initial authenticator distribution; * establishing and implementing administrative procedures for lost/compromised or damaged authenticators; * establishing and implementing administrative procedures for revoking authenticators; * changing default content of authenticators upon information system installation; * establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if deemed to be appropriate by the organization); * changing/refreshing authenticators in accordance with the organization-defined time period by authenticator type; * protecting authenticator content from unauthorized disclosure and modification; and * requiring users to take, and having devices implement, specific measures to safeguard authenticators. |  |

|  |  |  |
| --- | --- | --- |
| **IA-5(1)** | **AUTHENTICATOR MANAGEMENT – CONTROL ENHANCEMENT** | **RESULTS** |
| **IA-5(1).1** | Determine if: |  |
| **IA-5(1).1.1** | 1. the organization defines the minimum password complexity requirements to be enforced for case sensitivity, the number of characters, and the mix of upper-case letters, lower case letters, numbers, and special characters including minimum requirements for each type; |  |
| **IA-5(1).1.2** | 1. the organization defines the minimum number of characters that must be changed when new passwords are created; |  |
| **IA-5(1).1.3** | 1. the organization defines the restrictions to be enforced for password minimum lifetime and password maximum lifetime parameters; |  |
| **IA-5(1).1.4** | 1. the organization defines the number of generations for which password reuse is prohibited; and |  |
| **IA-5(1).1.5** | 1. the information system, for password-based authentication:  * enforces the minimum password complexity standards that meet the organization-defined requirements; * enforces the organization-defined minimum number of characters that must be changed when new passwords are created; * encrypts passwords in storage and in transmission; * enforces the organization-defined restrictions for password minimum lifetime and password maximum lifetime parameters; and * prohibits password reuse for the organization-defined number of generations. |  |

|  |  |  |
| --- | --- | --- |
| **IA-5(2)** | **AUTHENTICATOR MANAGEMENT – CONTROL ENHANCEMENT** | **RESULTS** |
| **IA-5(2).1** | Determine if the information system, for PKI-based authentication:   * validates certificates by constructing a certification path with status information with an accepted trust anchor; * enforces authorized access to the corresponding private key; and * maps the authenticated identity to the user account. |  |

|  |  |  |
| --- | --- | --- |
| **IA-5(3)** | **AUTHENTICATOR MANAGEMENT – CONTROL ENHANCEMENT** | **RESULTS** |
| **IA-5(3).1** | Determine if: |  |
| **IA-5(3).1.1** | 1. the organization defines the types of and/or specific authenticators for which the registration process must be carried out in person before a designated registration authority with authorization by a designated organizational official; and |  |
| **IA-5(3).1.2** | 1. the organization requires that the registration process to receive organization-defined types of and/or specific authenticators be carried out in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor). |  |

|  |  |  |
| --- | --- | --- |
| **IA-6** | **AUTHENTICATOR FEEDBACK** | **RESULTS** |
| **IA-6.1** | Determine if the information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals. |  |

|  |  |  |
| --- | --- | --- |
| **IA-7** | **CRYPTOGRAPHIC MODULE AUTHENTICATION** | **RESULTS** |
| **IA-7.1** | Determine if the information system employs authentication methods that meet the requirements of applicable laws, Executive Order, directive, policies, regulation, standards, and guidance for authentication to a cryptographic module (for non-national security systems, the cryptographic requirements are defined by FIPS 140-2, as amended). |  |

|  |  |  |
| --- | --- | --- |
| **IA-8** | **IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)** | **RESULTS** |
| **IA-8.1** | Determine if the information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users). |  |

### Incident Response (IR)

|  |  |  |
| --- | --- | --- |
| **IR-1** | **INCIDENT RESPONSE POLICY AND PROCEDURES** | **RESULTS** |
| **IR-1.1** | Determine if: |  |
| **IR-1.1.1** | 1. the organization develops and formally documents incident response policy; |  |
| **IR-1.1.2** | 1. the organization incident response policy addresses:  * purpose; * scope; * roles and responsibilities; * management commitment; * coordination among organizational entities; and * compliance; |  |
| **IR-1.1.3** | 1. the organization disseminates formal documented incident response policy to elements within the organization having associated incident response roles and responsibilities; |  |
| **IR-1.1.4** | 1. the organization develops and formally documents incident response procedures; |  |
| **IR-1.1.5** | 1. the organization incident response procedures facilitate implementation of the incident response policy and associated incident response controls; and |  |
| **IR-1.1.6** | 1. the organization disseminates formal documented incident response procedures to elements within the organization having associated incident response roles and responsibilities. |  |
| **IR-1.2** | Determine if: |  |
| **IR-1.2.1** | 1. the organization defines the frequency of incident response policy reviews/updates; |  |
| **IR-1.2.2** | 1. the organization reviews/updates incident response policy in accordance with organization-defined frequency; and |  |
| **IR-1.2.3** | 1. the organization defines the frequency of incident response procedure reviews/updates; |  |
| **IR-1.2.4** | 1. the organization reviews/updates incident response procedures in accordance with organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **IR-2** | **INCIDENT RESPONSE TRAINING** | **RESULTS** |
| **IR-2.1** | Determine if: |  |
| **IR-2.1.1** | 1. The organization identifies and documents personnel with incident response roles and responsibilities; |  |
| **IR-2.1.2** | 1. The organization provides incident response training to personnel with incident response roles and responsibilities; |  |
| **IR-2.1.2** | 1. Incident response training material addresses the procedures and activities necessary to fulfill identified organizational incident response roles and responsibilities; |  |
| **IR-2.1.2** | 1. The organization defines in the security plan, explicitly or by reference, the frequency of refresher incident response training and the frequency is at least annually; and |  |
| **IR-2.1.2** | 1. The organization provides refresher incident response training in accordance with organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **IR-3** | **INCIDENT RESPONSE TESTING AND EXERCISES** | **RESULTS** |
| **IR-3.1** | Determine if: |  |
| **IR-3.1.1** | 1. the organization defines in the security plan, explicitly or by reference, incident response test/exercises; |  |
| **IR-3.1.2** | 1. the organization defines in the security plan, explicitly or by reference, the frequency of incident response test/exercises and the frequency is at least annually; |  |
| **IR-3.1.3** | 1. the organization tests/exercises the incident response capability for the information system using organization-defined tests/exercises in accordance with organization defined frequency; |  |
| **IR-3.1.4** | 1. the organization documents the results of incident response test/exercises; and |  |
| **IR-3.1.5** | 1. the organization determines the effectiveness of the incident response capability. |  |

|  |  |  |
| --- | --- | --- |
| **IR-4** | **INCIDENT HANDLING** | **RESULTS** |
| **IR-4.1** | Determine if: |  |
| **IR-4.1.1** | 1. the organization implements and incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; and |  |
| **IR-4.1.2** | 1. the organization incorporates the lessons learned from ongoing incident handling activities into the incident response procedures and implements the procedures accordingly. |  |

|  |  |  |
| --- | --- | --- |
| **IR-4(1)** | **INCIDENT HANDLING – CONTROL ENHANCEMENT** | **RESULTS** |
| **IR-4(1).1** | Determine if the organization employs automated mechanisms to support the incident handling process. |  |

|  |  |  |
| --- | --- | --- |
| **IR-5** | **INCIDENT MONITORING** | **RESULTS** |
| **IR-5.1** | Determine if the organization tracks and documents information system security incidents on an ongoing basis. |  |

|  |  |  |
| --- | --- | --- |
| **IR-6** | **INCIDENT REPORTING** | **RESULTS** |
| **IR-6.1** | Determine if: |  |
| **IR-6.1.1** | 1. the organization promptly reports incident information to appropriate authorities; |  |
| **IR-6.1.2** | 1. incident reporting is consistent with NIST Special Publication 800-61; |  |
| **IR-6.1.3** | 1. the types of incident information reported, the content and timeliness of the reports, and the list of designated reporting authorities or organizations is consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance; and |  |
| **IR-6.1.4** | 1. weakness and vulnerabilities in the information system are reported to appropriate organizational officials in a timely manner to prevent security incidents. |  |

|  |  |  |
| --- | --- | --- |
| **IR-6(1)** | **INCIDENT REPORTING – CONTROL ENHANCEMENT** | **RESULTS** |
| **IR-6(1).1** | Determine if the organization employs automated mechanisms to assist in the reporting of security incidents. |  |

|  |  |  |
| --- | --- | --- |
| **IR-7** | **INCIDENT RESPONSE ASSISTANCE** | **RESULTS** |
| **IR-7.1** | Determine if: |  |
| **IR-7.1.1** | 1. the organization provides and incident response support resource that offers advice and assistance to user of the information system for the handling and reporting of security incidents; and |  |
| **IR-7.1.2** | 1. the incident response support resources is an integral parts of the organization’s incident response capability. |  |

|  |  |  |
| --- | --- | --- |
| **IR-7(1)** | **INCIDENT RESPONSE ASSISTANCE – CONTROL ENHANCEMENT** | **RESULTS** |
| **IR-7(1).1** | Determine if the organization employs automated mechanisms to increase the availability of incident response-related information and support. |  |

|  |  |  |
| --- | --- | --- |
| **IR-8** | **INCIDENT RESPONSE PLAN** | **RESULTS** |
| **IR-8.1** | Determine if: |  |
| **IR-8.1.1** | 1. the organization develops an incident response plan that:   - provides the organization with a roadmap for implementing its incident response  capability;  - describes the structure and organization of the incident response capability;  - provides a high-level approach for how the incident response capability fits into the  overall organization;  - meets the unique requirements of the organization, which relate to mission, size,  structure, and functions;  - defines reportable incidents;  - provides metrics for measuring the incident response capability within the organization;  - defines the resources and management support needed to effectively maintain and mature an incident response capability; and  - is reviewed and approved by designated officials within the organization. |  |
| **IR-8.1.2** | 1. the organization defines, in the incident response plan, incident response personnel   (identified by name and/or role) and organizational elements;  (ii) the organization distributes copies of the incident response plan to incident  response personnel and organizational elements identified in the plan;  (iii) the organization defines, in the incident response plan, the frequency to review the  plan;  (iv) the organization reviews the incident response plan in accordance with the  organization-defined frequency;  (v) the organization revises the incident response plan to address system/organizational  changes or problems encountered during plan implementation, execution, or  testing; and  (vi) the organization communicates incident response plan changes to incident response  personnel and organizational elements identified in the plan. |  |

### Maintenance (MA)

|  |  |  |
| --- | --- | --- |
| **MA-1** | **SYSTEM MAINTENANCE POLICY AND PROCEDURES** | **RESULTS** |
| **MA-1.1** | Determine if: |  |
| **MA-1.1.1** | 1. the organization develops and formally documents system maintenance policy; |  |
| **MA-1.1.2** | 1. the organization system maintenance policy addresses:  * purpose; * scope; * roles and responsibilities; * management commitment; * coordination among organizational entities; and * compliance; |  |
| **MA-1.1.3** | 1. the organization disseminates formal documented system maintenance policy to elements within the organization having associated system maintenance roles and responsibilities; |  |
| **MA-1.1.4** | 1. the organization develops and formally documents system maintenance procedures; |  |
| **MA-1.1.5** | 1. the organization system maintenance procedures facilitate implementation of the system maintenance policy and associated system maintenance controls; and |  |
| **MA-1.1.6** | 1. the organization disseminates formal documented system maintenance procedures to elements within the organization having associated system maintenance roles and responsibilities. |  |
| **MA-1.2** | Determine if: |  |
| **MA-1.2.1** | 1. the organization defines the frequency of system maintenance policy reviews/updates; |  |
| **MA-1.2.2** | 1. the organization reviews/updates system maintenance policy in accordance with organization-defined frequency; and |  |
| **MA-1.2.3** | 1. the organization defines the frequency of system maintenance procedure reviews/updates; |  |
| **MA-1.2.4** | 1. the organization reviews/updates system maintenance procedures in accordance with organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **MA-2** | **CONTROLLED MAINTENANCE** | **RESULTS** |
| **MA-2.1** | Determine if: |  |
| **MA-2.1.1** | 1. the organization schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements; |  |
| **MA-2.1.2** | 1. the organization controls all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location; |  |
| **MA-2.1.3** | 1. the organization requires that a designated official explicitly approve the removal of the information system or system components from organizational facilities for offsite maintenance or repairs; |  |
| **MA-2.1.4** | 1. the organization sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; and |  |
| **MA-2.1.5** | 1. the organization checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions. |  |

|  |  |  |
| --- | --- | --- |
| **MA-2(1)** | **CONTROLLED MAINTENANCE – CONTROL ENHANCEMENT** | **RESULTS** |
| **MA-2(1).1** | Determine if the organization maintains maintenance records for the information system  that include:   * date and time of maintenance; * name of the individual performing the maintenance; * name of escort, if necessary; * a description of the maintenance performed; and * a list of equipment removed or replaced (including identification numbers, if applicable). |  |

|  |  |  |
| --- | --- | --- |
| **MA-3** | **MAINTENANCE TOOLS** | **RESULTS** |
| **MA-3.1** | Determine if: |  |
| **MA-3.1.1** | 1. the organization approves, controls, and monitors the use of information system maintenance tools; and |  |
| **MA-3.1.2** | 1. the organization maintains maintenance tools on an ongoing basis. |  |

|  |  |  |
| --- | --- | --- |
| **MA-3(1)** | **MAINTENANCE TOOLS – CONTROL ENHANCEMENT** | **RESULTS** |
| **MA-3(1).1** | Determine if the organization inspects all maintenance tools carried into a facility by maintenance personnel for obvious improper modifications. |  |

|  |  |  |
| --- | --- | --- |
| **MA-3(2)** | **MAINTENANCE TOOLS – CONTROL ENHANCEMENT** | **RESULTS** |
| **MA-3(2).1** | Determine if the organization checks all media containing diagnostic and test programs for malicious code before the media are used in the information system. |  |

|  |  |  |
| --- | --- | --- |
| **MA-4** | **NON-LOCAL MAINTENANCE** | **RESULTS** |
| **MA-4.1** | Determine if: |  |
| **MA-4.1.1** | 1. the organization authorizes, monitors, and controls the executions of maintenance and diagnostic activities conducted remotely by individuals communication through an external, non-organization-controlled network (e.g., the internet) , if employed; |  |
| **MA-4.1.2** | 1. the organization documents in the security plan, the remote maintenance and diagnostic tools to be employed; |  |
| **MA-4.1.3** | 1. the organization maintains records for all remote maintenance and diagnostic activities; |  |
| **MA-4.1.4** | 1. the organization (or information system in certain cases) terminates all sessions and remote connections invoked in the performance of remote maintenance and diagnostic activity when the remote maintenance or diagnostics is completed.; and |  |
| **MA-4.1.5** | 1. the organization changes the passwords following each remote maintenance and diagnostic activity if password-based authentication is used to accomplish remote maintenance. |  |

|  |  |  |
| --- | --- | --- |
| **MA-4(1)** | **NON-LOCAL MAINTENANCE – CONTROL ENHANCEMENT** | **RESULTS** |
| **MA-4(1).1** | Determine if: |  |
| **MA-4(1).1.1** | 1. the organization audits non-local maintenance and diagnostic sessions; and |  |
| **MA-4(1).1.2** | 1. designated organizational personnel review the maintenance records of the sessions. |  |

|  |  |  |
| --- | --- | --- |
| **MA-4(2)** | **NON-LOCAL MAINTENANCE – CONTROL ENHANCEMENT** | **RESULTS** |
| **MA-4(2).1** | Determine if the organization documents the installation and use of non-local maintenance and diagnostic connections in the security plan for the information system. |  |

|  |  |  |
| --- | --- | --- |
| **MA-5** | **MAINTENANCE PERSONNEL** | **RESULTS** |
| **MA-5.1** | Determine if: |  |
| **MA-5.1.1** | 1. the organization allows only authorized personnel to perform maintenance on the information system; and |  |
| **MA-5.1.2** | 1. the organization supervises authorized maintenance personnel who do not have needed access authorizations to the information system during the performance of maintenance activities on the system using organizational personnel with appropriate access authorizations. |  |

|  |  |  |
| --- | --- | --- |
| **MA-6** | **TIMELY MAINTENANCE** | **RESULTS** |
| **MA-6.1** | Determine if: |  |
| **MA-6.1.1** | 1. the organization defines in the security plan, explicitly or by reference, key information system components; |  |
| **MA-6.2.1** | 1. the organization defines in the security plan, explicitly or by reference, the time period within which support and spare parts mush be obtained after a failure; and |  |
| **MA-6.3.1** | 1. the organization obtains maintenance support and spare parts for the organization-defined list of key information system components within the organization-defined time period of failure. |  |

### Media Protection (MP)

|  |  |  |
| --- | --- | --- |
| **MP-1** | **MEDIA PROTECTION POLICY AND PROCEDURES** | **RESULTS** |
| **MP-1.1** | Determine if: |  |
| **MP-1.1.1** | 1. the organization develops and formally documents media protection policy; |  |
| **MP-1.1.2** | 1. the organization media protection policy addresses:  * purpose; * scope; * roles and responsibilities; * management commitment; * coordination among organizational entities; and * compliance; |  |
| **MP-1.1.3** | 1. the organization disseminates formal documented media protection policy to elements within the organization having associated media protection roles and responsibilities; |  |
| **MP-1.1.4** | 1. the organization develops and formally documents media protection procedures; |  |
| **MP-1.1.5** | 1. the organization media protection procedures facilitate implementation of the media protection policy and associated media protection controls; and |  |
| **MP-1.1.6** | 1. the organization disseminates formal documented media protection procedures to elements within the organization having associated media protection roles and responsibilities. |  |
| **MP-1.2** | Determine if: |  |
| **MP-1.2.1** | 1. the organization defines the frequency of media protection policy reviews/updates; |  |
| **MP-1.2.2** | 1. the organization reviews/updates media protection policy in accordance with organization-defined frequency; and |  |
| **MP-1.2.3** | 1. the organization defines the frequency of media protection procedure reviews/updates; |  |
| **MP-1.2.4** | 1. the organization reviews/updates media protection procedures in accordance with organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **MP-2** | **MEDIA ACCESS** | **RESULTS** |
| **MP-2.1** | Determine if the organization restricts access to information system media to authorized users. |  |

|  |  |  |
| --- | --- | --- |
| **MP-2(1)** | **MEDIA ACCESS – CONTROL ENHANCEMENT** | **RESULTS** |
| **MP-2(1).1** | Determine if: |  |
| **MP-2(1).1.1** | 1. the organization employs automated mechanisms to restrict access to media storage areas; and |  |
| **MP-2(1).1.2** | 1. the organization employs automated mechanisms to audit access attempts and access granted. |  |

|  |  |  |
| --- | --- | --- |
| **MP-3** | **MEDIA MARKING** | **RESULTS** |
| **MP-3.1** | Determine if the organization: |  |
| **MP-3.1.1** | 1. defines removable media types and information system output that require marking; |  |
| **MP-3.1.2** | 1. marks removable media and information system output in accordance with organizational policies and procedures, indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; |  |
| **MP-3.1.3** | 1. defines:  * removable media types and information system output exempt from marking; * controlled areas designated for retaining removable media and information output exempt from marking; and |  |
| **MP-3.1.4** | 1. removable media and information system output exempt from marking remain within designated controlled areas. |  |

|  |  |  |
| --- | --- | --- |
| **MP-4** | **MEDIA STORAGE** | **RESULTS** |
| **MP-4.1** | Determine if: |  |
| **MP-4.1.1** | 1. the organization selects and documents the media and associated information contained on that media requiring physical protection in accordance with an organizational assessment of risk; |  |
| **MP-4.1.2** | 1. the organization defines the specific measures used to protect the selected media and information contained on that media; |  |
| **MP-4.1.3** | 1. the organization physically controls and securely stores information system media within controlled areas; and |  |
| **MP-4.1.4** | 1. the organization protects information system media commensurate with the FIPS 199 security categorization of the information contained on the media. |  |

|  |  |  |
| --- | --- | --- |
| **MP-5** | **MEDIA TRANSPORT** | **RESULTS** |
| **MP-5.1** | Determine if: |  |
| **MP-5.1.1** | 1. the organization identifies personnel authorized to transport information system media outside of controlled area; |  |
| **MP-5.1.2** | 1. the organization documents, in policy and procedures, the media requiring protection during transport and the specific measures taken to protect such transported media; |  |
| **MP-5.1.3** | 1. the organization protects and controls information system media during transport outside of controlled areas; and |  |
| **MP-5.1.4** | 1. the organization restricts the activities associated with transport of information system media to authorized personnel. |  |

|  |  |  |
| --- | --- | --- |
| **MP-5(2)** | **MEDIA TRANSPORT – CONTROL ENHANCEMENT** | **RESULTS** |
| **MP-5(2).1** | Determine if the organization documents, where appropriate, activities associated with the transport of information system media using the organization-defined system of records. |  |

|  |  |  |
| --- | --- | --- |
| **MP-5(4)** | **MEDIA TRANSPORT – CONTROL ENHANCEMENT** | **RESULTS** |
| **MP-5(4).1** | Determine if the organization employs cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas. |  |

|  |  |  |
| --- | --- | --- |
| **MP-6** | **MEDIA SANITIZATION** | **RESULTS** |
| **MP-6.1** | Determine if: |  |
| **MP-6.1.1** | 1. the organization identifies information system media requiring sanitization and the appropriate sanitization techniques and procedures to be used in t process; |  |
| **MP-6.1.2** | 1. the organization sanitizes identified information system media, both paper and digital, prior to disposal or release for reuse; and |  |
| **MP-6.1.3** | 1. information system media sanitation is consistent with NIST Special Publication 800-88. |  |

### Physical and Environmental Protection (PE)

|  |  |  |
| --- | --- | --- |
| **PE-1** | **PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES** | **RESULTS** |
| **PE-1.1** | Determine if: |  |
| **PE-1.1.1** | 1. the organization develops and formally documents physical and environmental protection policy; |  |
| **PE-1.1.2** | 1. the organization physical and environmental protection policy addresses:  * purpose; * scope; * roles and responsibilities; * management commitment; * coordination among organizational entities; and * compliance; |  |
| **PE-1.1.3** | 1. the organization disseminates formal documented physical and environmental protection policy to elements within the organization having associated physical and environmental protection roles and responsibilities; |  |
| **PE-1.1.4** | 1. the organization develops and formally documents physical and environmental protection procedures; |  |
| **PE-1.1.5** | 1. the organization physical and environmental protection procedures facilitate implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and |  |
| **PE-1.1.6** | 1. the organization disseminates formal documented physical and environmental protection procedures to elements within the organization having associated physical and environmental protection roles and responsibilities. |  |
| **PE-1.2** | Determine if: |  |
| **PE-1.2.1** | 1. the organization defines the frequency of physical and environmental protection policy reviews/updates; |  |
| **PE-1.2.2** | 1. the organization reviews/updates physical and environmental protection policy in accordance with organization-defined frequency; and |  |
| **PE-1.2.3** | 1. the organization defines the frequency of physical and environmental protection procedure reviews/updates; |  |
| **PE-1.2.4** | 1. the organization reviews/updates physical and environmental protection procedures in accordance with organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **PE-2** | **PHYSICAL ACCESS AUTHORIZATIONS** | **RESULTS** |
| **PE-2.1** | Determine if: |  |
| **PE-2.1.1** | 1. the organization identifies areas within the facility that are publicly accessible; |  |
| **PE-2.1.2** | 1. the organization develops and keeps current lists of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); and |  |
| **PE-2.1.3** | 1. the organization issues appropriate authorization credentials (e.g., badges, identification cards, smart cards). |  |
| **PE-2.2** | Determine if: |  |
| **PE-2.2.1** | 1. the organization defines the frequency for review and approval of the physical access list and authorization credentials for the facility; |  |
| **PE-2.2.2** | 1. organization reviews and approves the access list and authorization credentials in accordance with the organization-defined frequency; and |  |
| **PE-2.2.3** | 1. the organization removes from the access list personnel no longer requiring access. |  |

|  |  |  |
| --- | --- | --- |
| **PE-3.1** | Determine if: | **RESULTS** |
| **PE-3.1.1** | 1. the organization enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible); |  |
| **PE-3.1.2** | 1. the organization verifies individual access authorizations before granting access to the facility; |  |
| **PE-3.1.3** | 1. the organization controls entry to the facility containing the information system using physical access devices (e.g., keys, locks, combinations, card readers) and/or guards; |  |
| **PE-3.1.4** | 1. the organization controls access to areas officially designated as publicly accessible in accordance with the organization’s assessment of risk; and |  |
| **PE-3.1.5** | 1. the organization secures keys, combinations, and other physical access devices. |  |

|  |  |  |
| --- | --- | --- |
| **PE-4** | **ACCESS CONTROL FOR TRANSMISSION MEDIUM** | **RESULTS** |
| **PE-4.1** | Determine if the organization controls physical access to information system distribution and transmission lines within organizational facilities. |  |

|  |  |  |
| --- | --- | --- |
| **PE-5** | **ACCESS CONTROL FOR DISPLAY MEDIUM** | **RESULTS** |
| **PE-5.1** | Determine if the organization controls physical access to information system devices that display information to prevent unauthorized individuals from observing the display output. |  |

|  |  |  |
| --- | --- | --- |
| **PE-6** | **MONITORING PHYSICAL ACCESS** | **RESULTS** |
| **PE-6.1** | Determine if: |  |
| **PE-6.1.1** | 1. the organization monitors physical access to the information system to detect and respond to physical security incidents; |  |
| **PE-6.1.2** | 1. the organization defines the frequency to review physical access logs; |  |
| **PE-6.1.3** | 1. the organization reviews physical access logs in accordance with the organization-defined frequency; and |  |
| **PE-6.1.4** | 1. the organization coordinates results of reviews and investigations with the organization’s incident response capability. |  |

|  |  |  |
| --- | --- | --- |
| **PE-6(1)** | **MONITORING PHYSICAL ACCESS – CONTROL ENHANCEMENT** | **RESULTS** |
| **PE-6(1).1** | Determine if the organization monitors real-time intrusion alarms and surveillance equipment. |  |

|  |  |  |
| --- | --- | --- |
| **PE-7** | **VISITOR CONTROL** | **RESULTS** |
| **PE-7.1** | Determine if the organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other that areas designated a publicly accessible. |  |

|  |  |  |
| --- | --- | --- |
| **PE-7(1)** | **VISITOR CONTROL – CONTROL ENHANCEMENT** | **RESULTS** |
| **PE-7(1).1** | Determine if the organization escorts visitors and monitors visitor activity, when required. |  |

|  |  |  |
| --- | --- | --- |
| **PE-8** | **ACCESS RECORDS** | **RESULTS** |
| **PE-8.1** | Determine if: |  |
| **PE-8.1.1** | 1. the organization maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); |  |
| **PE-8.1.2** | 1. the organization defines the frequency to review visitor access records; |  |
| **PE-8.1.3** | 1. the organization reviews the visitor access records in accordance with the organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **PE-9** | **POWER EQUIPMENT AND POWER CABLING** | **RESULTS** |
| **PE-9.1** | Determine if the organization protects power equipment and power cabling for the information system from damage and destruction. |  |

|  |  |  |
| --- | --- | --- |
| **PE-10** | **EMERGENCY SHUTOFF** | **RESULTS** |
| **PE-10.1** | Determine if: |  |
| **PE-10.1.1** | 1. the organization provides the capability of shutting off power to the information system or individual system components in emergency situations; |  |
| **PE-10.1.2** | 1. the organization defines the location of emergency shutoff switches or devices by information system or system component; |  |
| **PE-10.1.3** | 1. the organization places emergency shutoff switches or devices in an organization-defined location by information system or system component to facilitate safe and easy access for personnel; and |  |
| **PE-10.1.4** | 1. the organization protects the emergency power shutoff capability from unauthorized activation. |  |

|  |  |  |
| --- | --- | --- |
| **PE-11** | **EMERGENCY POWER** | **RESULTS** |
| **PE-11.1** | Determine if the organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss. |  |

|  |  |  |
| --- | --- | --- |
| **PE-12** | **EMERGENCY LIGHTING** | **RESULTS** |
| **PE-12.1** | Determine if: |  |
| **PE-12.1.1** | 1. the organization employs automatic emergency lighting for the information system that activates in the event of a power outage or disruption; |  |
| **PE-12.1.2** | 1. the organization employs automatic emergency lighting for the information system that covers emergency exits and evacuation routes within the facility; and |  |
| **PE-12.1.3** | 1. the organization maintains the automatic emergency lighting for the information system. |  |

|  |  |  |
| --- | --- | --- |
| **PE-13** | **FIRE PROTECTION** | **RESULTS** |
| **PE-13.1** | Determine if: |  |
| **PE-13.1.1** | 1. the organization employs fire suppression and detection devices/systems for the information system that are supported by an independent energy source; and |  |
| **PE-13.1.2** | 1. the organization maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source. |  |

|  |  |  |
| --- | --- | --- |
| **PE-13(1)** | **FIRE PROTECTION – CONTROL ENHANCEMENT** | **RESULTS** |
| **PE-13(1).1** | Determine if the organization employs fire detection devices/systems for the information system that, without manual intervention, activate automatically and notify the organization and emergency responders in the event of a fire. |  |

|  |  |  |
| --- | --- | --- |
| **PE-13(2)** | **FIRE PROTECTION – CONTROL ENHANCEMENT** | **RESULTS** |
| **PE-13(2).1** | Determine if the organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation to the organization and emergency responders. |  |

|  |  |  |
| --- | --- | --- |
| **PE-13(3)** | **FIRE PROTECTION – CONTROL ENHANCEMENT** | **RESULTS** |
| **PE-13(3).1** | Determine if the organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis. |  |

|  |  |  |
| --- | --- | --- |
| **PE-14** | **TEMPERATURE AND HUMIDITY CONTROLS** | **RESULTS** |
| **PE-14.1** | Determine if: |  |
| **PE-14.1.1** | 1. the organization defines the acceptable temperature and humidity levels within the facility where the information system resides; |  |
| **PE-14.1.2** | 1. the organization maintains temperature and humidity levels within the facility where the information system resides in accordance with organization-defined acceptable levels; |  |
| **PE-14.1.3** | 1. the organization defines the frequency to monitor temperature and humidity levels; and |  |
| **PE-14.1.4** | 1. the organization monitors the temperature and humidity levels within the facility where the information system resides in accordance with the organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **PE-15** | **WATER DAMAGE PROTECTION** | **RESULTS** |
| **PE-15.1** | Determine if: |  |
| **PE-15.1.1** | 1. the organization protects the information system from damage resulting from water leakage by providing master shutoff valves that are accessible and working properly; and |  |
| **PE-15.1.2** | 1. key personnel within the organization have knowledge of the master water shutoff valves. |  |

|  |  |  |
| --- | --- | --- |
| **PE-16** | **DELIVERY AND REMOVAL** | **RESULTS** |
| **PE-16.1** | Determine if: |  |
| **PE-16.1.1** | 1. the organization defines the types of information system components to be authorized, monitored, and controlled as such components are entering or exiting the facility; |  |
| **PE-16.1.2** | 1. the organization authorizes, monitors, and controls organization-defined information system components entering and exiting the facility; and |  |
| **PE-16.1.3** | 1. the organization maintains records of information system components entering and exiting the facility. |  |

|  |  |  |
| --- | --- | --- |
| **PE-17** | **ALTERNATE WORK SITE** | **RESULTS** |
| **PE-17.1** | Determine if: |  |
| **PE-17.1.1** | 1. the organization defines the management, operational, and technical information system security controls to be employed at alternate work sites; |  |
| **PE-17.1.2** | 1. the organization employs organization-defined management, operational, and technical information system security controls at alternate work sites; |  |
| **PE-17.1.3** | 1. the organization assesses, as feasible, the effectiveness of security controls at alternate work sites; and |  |
| **PE-17.1.4** | 1. the organization provides a means for employees to communicate with information security personnel in case of security incidents or problems. |  |

|  |  |  |
| --- | --- | --- |
| **PE-18** | **LOCATION OF INFORMATION SYSTEM COMPONENTS** | **RESULTS** |
| **PE-18.1** | Determine if: |  |
| **PE-18.1.1** | 1. the organization positions information system components within the facility to minimize potential damage from physical and environmental hazards; and |  |
| **PE-18.2.1** | 1. the organization positions information system components within the facility to minimize the opportunity for unauthorized access. |  |

### Planning (PL)

|  |  |  |
| --- | --- | --- |
| **PL-1** | **SECURITY PLANNING POLICY AND PROCEDURES** | **RESULTS** |
| **PL-1.1** | Determine if: |  |
| **PL-1.1.1** | 1. the organization develops and formally documents security planning policy; |  |
| **PL-1.1.2** | 1. the organization security planning policy addresses:  * purpose; * scope; * roles and responsibilities; * management commitment; * coordination among organizational entities; and * compliance; |  |
| **PL-1.1.3** | 1. the organization disseminates formal documented security planning policy to elements within the organization having associated security planning roles and responsibilities; |  |
| **PL-1.1.4** | 1. the organization develops and formally documents security planning procedures; |  |
| **PL-1.1.5** | 1. the organization security planning procedures facilitate implementation of the security planning policy and associated security planning controls; and |  |
| **PL-1.1.6** | 1. the organization disseminates formal documented security planning procedures to elements within the organization having associated security planning roles and responsibilities. |  |
| **PL-1.2** | Determine if: |  |
| **PL-1.2.1** | 1. the organization defines the frequency of security planning policy reviews/updates; |  |
| **PL-1.2.2** | 1. the organization reviews/updates security planning policy in accordance with organization-defined frequency; and |  |
| **PL-1.2.3** | 1. the organization defines the frequency of security planning procedure reviews/updates; |  |
| **PL-1.2.4** | 1. the organization reviews/updates security planning procedures in accordance with organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **PL-2** | **SYSTEM SECURITY PLAN** | **RESULTS** |
| **PL-2.1** | Determine if: |  |
| **PL-2.1.1** | 1. the organization develops and implements a security plan for the information system; |  |
| **PL-2.1.2** | 1. the security plan provides and overview of the security requirements for the information system and a description of the security controls planned r in place for meeting the security requirements; |  |
| **PL-2.1.3** | 1. the organizations defines in the security plan, explicitly or by reference, the values for all organization-defined parameters (i.e., assignment and selection operations) in applicable security controls and control enhancements; |  |
| **PL-2.1.4** | 1. the security plan development is consistent with NIST Special Publication 800-18; |  |
| **PL-2.1.5** | 1. the security plan is consistent with the organization’s information system architecture and information security architecture; and |  |
| **PL-2.1.6** | 1. designated organizational officials review and approve the security plan. |  |

|  |  |  |
| --- | --- | --- |
| **PL-4** | **RULES OF BEHAVIOR** | **RESULTS** |
| **PL-4.1** | Determine if: |  |
| **PL-4.1.1** | 1. the organization establishes a set of rules that describe user responsibilities and expected behavior with regard to information and information system usage; |  |
| **PL-4.2.1** | 1. the organization makes the rules available to all information system users; |  |
| **PL-4.3.1** | 1. the rules of behavior for organizational personnel are consistent with NIST Special Publication 800-18; and |  |
| **PL-4.4.1** | 1. the organization receives a signed acknowledgement from user’s indication that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information. |  |

|  |  |  |
| --- | --- | --- |
| **PL-5** | **PRIVACY IMPACT ASSESSMENT** | **RESULTS** |
| **PL-5.1** | Determine if: |  |
| **PL-5.1.1** | 1. the organization conducts a privacy impact assessment on the information system; and |  |
| **PL-5.1.2** | 1. the privacy impact assessment is compliant with OMB policy. |  |

|  |  |  |
| --- | --- | --- |
| **PL-6** | **SECURITY-RELATED ACTIVITY PLANNING** | **RESULTS** |
| **PL-6.1** | Determine if: |  |
| **PL-6.1.1** | 1. the organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations, organizational assets, and individuals; and |  |
| **PL-6.2.1** | 1. the organization’s advance planning and coordination of security-related activities includes both emergency and non-emergency situations. |  |

### Personnel Security (PS)

|  |  |  |
| --- | --- | --- |
| **PS-1** | **PERSONNEL SECURITY POLICY AND PROCEDURES** | **RESULTS** |
| **PS-1.1** | Determine if: |  |
| **PS-1.1.1** | 1. the organization develops and formally documents personnel security policy; |  |
| **PS-1.1.2** | 1. the organization personnel security policy addresses:  * purpose; * scope; * roles and responsibilities; * management commitment; * coordination among organizational entities; and * compliance; |  |
| **PS-1.1.3** | 1. the organization disseminates formal documented personnel security policy to elements within the organization having associated personnel security roles and responsibilities; |  |
| **PS-1.1.4** | 1. the organization develops and formally documents personnel security procedures; |  |
| **PS-1.1.5** | 1. the organization personnel security procedures facilitate implementation of the personnel security policy and associated personnel security controls; and |  |
| **PS-1.1.6** | 1. the organization disseminates formal documented personnel security procedures to elements within the organization having associated personnel security roles and responsibilities. |  |
| **PS-1.2** | Determine if: |  |
| **PS-1.2.1** | 1. the organization defines the frequency of personnel security policy reviews/updates; |  |
| **PS-1.2.2** | 1. the organization reviews/updates personnel security policy in accordance with organization-defined frequency; and |  |
| **PS-1.2.3** | 1. the organization defines the frequency of personnel security procedure reviews/updates; |  |
| **PS-1.2.4** | 1. the organization reviews/updates personnel security procedures in accordance with organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **PS-2** | **POSITION CATEGORIZATION** | **RESULTS** |
| **PS-2.1** | Determine if: |  |
| **PS-2.1.1** | 1. the organization assigns a risk designations to all positions within the organization; |  |
| **PS-2.1.2** | 1. the organization establishes a screening criteria for individuals filling organizational positions; |  |
| **PS-2.1.3** | 1. the risk designations for the organizational positions are consistent with 5 CFR 731.106(a) and OPM policy and guidance; |  |
| **PS-2.1.4** | 1. the organization defines in the security plan, explicitly or by reference, the frequency of risk designation reviews and updates for organizational positions; and |  |
| **PS-2.1.5** | 1. the organization reviews and revises position risk designations in accordance with the organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **PS-3** | **PERSONNEL SCREENING** | **RESULTS** |
| **PS-3.1** | Determine if: |  |
| **PS-3.1.1** | 1. the organization screens individuals requiring access to organizational information and information systems prior to authorizing access; and |  |
| **PS-3.1.2** | 1. the personnel screening is consistent with 5 CFR 731.106, OPM policy, regulations, and guidance, FIPS 201 and NIST Special publications 800-73, 800-76, and 800-78, and the criteria established for the risk designation for the assigned position. |  |

|  |  |  |
| --- | --- | --- |
| **PS-4** | **PERSONNEL TERMINATION** | **RESULTS** |
| **PS-4.1** | Determine if: |  |
| **PS-4.1.1** | 1. the organization terminates information system access upon termination of individual employment; |  |
| **PS-4.2.1** | 1. the organization conducts exit interviews of terminated personnel; |  |
| **PS-4.3.1** | 1. the organization retrieves all organizational information system-related property from terminated personnel; and |  |
| **PS-4.4.1** | 1. the organization retains access to official documents and records on organizational information systems created by terminated personnel. |  |

|  |  |  |
| --- | --- | --- |
| **PS-5** | **PERSONNEL TRANSFER** | **RESULTS** |
| **PS-5.1** | Determine if: |  |
| **PS-5.1.1** | 1. the organization reviews information systems/facilities access authorizations when personnel are reassigned or transferred to other positions within the organization; and |  |
| **PS-5.1.2** | 1. the organization initiates appropriate actions (e.g., reissuing keys, identification cards, building passes; closing old accounts and establishing new accounts; and changing system access authorization) for personnel reassigned or transferred within the organization. |  |

|  |  |  |
| --- | --- | --- |
| **PS-6** | **ACCESS AGREEMENTS** | **RESULTS** |
| **PS-6.1** | Determine if: |  |
| **PS-6.1.1** | 1. the organization requires appropriate access agreements for individuals requiring access to organizational information and information systems before authorizing access; |  |
| **PS-6.2.1** | 1. the organization personnel sign appropriate access agreements prior to receiving access; |  |
| **PS-6.3.1** | 1. the organization defines in the security plan, explicitly or by reference, the frequency of reviews/updates the access agreements; and |  |
| **PS-6.4.1** | 1. the organization reviews/updates the access agreements in accordance with the organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **PS-7** | **THIRD-PARTY PERSONNEL SECURITY** | **RESULTS** |
| **PS-7.1** | Determine if: |  |
| **PS-7.1.1** | 1. the organization establishes personnel security requirements, including security roles and responsibilities, for third-party providers (e.g., service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, network and security management); |  |
| **PS-7.2.1** | 1. the organization explicitly includes personnel security requirements in acquisition-related documents in accordance with NIST Special Publication 800-35; and |  |
| **PS-7.3.1** | 1. the organization monitors third-party provider compliance with personnel security requirements. |  |

|  |  |  |
| --- | --- | --- |
| **PS-8** | **PERSONNEL SANCTIONS** | **RESULTS** |
| **PS-8.1** | Determine if: |  |
| **PS-8.1.1** | 1. the organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures; and |  |
| **PS-8.1.2** | 1. the personnel sanctions process is consistent with applicable laws, Executive Orders, directive, policies, regulations, standards, and guidance. |  |

### Risk Assessment (RA)

|  |  |  |
| --- | --- | --- |
| **RA-1** | **RISK ASSESSMENT POLICY AND PROCEDURES** | **RESULTS** |
| **RA-1.1** | Determine if: |  |
| **RA-1.1.1** | 1. the organization develops and formally documents risk assessment policy; |  |
| **RA-1.1.2** | 1. the organization risk assessment policy addresses:  * purpose; * scope; * roles and responsibilities; * management commitment; * coordination among organizational entities; and * compliance; |  |
| **RA-1.1.3** | 1. the organization disseminates formal documented risk assessment policy to elements within the organization having associated risk assessment roles and responsibilities; |  |
| **RA-1.1.4** | 1. the organization develops and formally documents risk assessment procedures; |  |
| **RA-1.1.5** | 1. the organization risk assessment procedures facilitate implementation of the risk assessment policy and associated risk assessment controls; and |  |
| **RA-1.1.6** | 1. the organization disseminates formal documented risk assessment procedures to elements within the organization having associated risk assessment roles and responsibilities. |  |
| **RA-1.2** | Determine if: |  |
| **RA-1.2.1** | 1. the organization defines the frequency of risk assessment policy reviews/updates; |  |
| **RA-1.2.2** | 1. the organization reviews/updates risk assessment policy in accordance with organization-defined frequency; and |  |
| **RA-1.2.3** | 1. the organization defines the frequency of risk assessment procedure reviews/updates; |  |
| **RA-1.2.4** | 1. the organization reviews/updates risk assessment procedures in accordance with organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **RA-2** | **SECURITY CATEGORIZATION** | **RESULTS** |
| **RA-2.1** | Determine if: |  |
| **RA-2.1.1** | 1. the organization conducts the security categorization of the information system as an organization-wide exercise with the involvement of senior-level officials, information system owners, chief information officer, senior agency information security officer, an mission/information owners; |  |
| **RA-2.1.2** | 1. the security categorization is consistent with FIPS 199 and considers the provisional impact levels and special factors in NIST Special Publication 800-60; |  |
| **RA-2.1.3** | 1. the organization considers in the security categorization of the information system, potential impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level impacts; |  |
| **RA-2.1.4** | 1. the organization includes supporting rationale for impact-level decisions as part of the security categorization; and |  |
| **RA-2.1.5** | 1. designated senior-level organizational officials review and approve the security categorizations. |  |

|  |  |  |
| --- | --- | --- |
| **RA-3** | **RISK ASSESSMENT** | **RESULTS** |
| **RA-3.1** | Determine if: |  |
| **RA-3.1.1** | 1. the organization assess the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support its operations and assets (including information and information systems managed/operated by external parties); and |  |
| **RA-3.1.2** | 1. the risk assessment is consistent with the NIST Special publication 800-30. |  |

|  |  |  |
| --- | --- | --- |
| **RA-5** | **VULNERABILITY SCANNING** | **RESULTS** |
| **RA-5.1** | Determine if: |  |
| **RA-5.1.1** | 1. the organization defines in the security plan, explicitly or by reference, the frequency of vulnerability scans within the information system; |  |
| **RA-5.1.2** | 1. the organization scans for vulnerabilities in the information system in accordance with the organization-defined frequency and/or random in accordance with organizational policy and assessment of risk, or when significant new vulnerabilities potentially affecting the system are identified and reported; |  |
| **RA-5.1.3** | 1. the organization uses appropriate scanning tools and techniques to conduct the vulnerability scans; |  |
| **RA-5.1.4** | 1. the organization trains selected personnel in the use and maintenance of vulnerability scanning tools and techniques; and |  |
| **RA-5.1.5** | 1. the organization freely shares the information obtained from the vulnerability scanning process with appropriate personnel throughout the organization to help eliminate similar vulnerabilities in other information systems. |  |

|  |  |  |
| --- | --- | --- |
| **RA-5(1)** | **VULNERABILITY SCANNING – CONTROL ENHANCEMENT** | **RESULTS** |
| **RA-5(1).1** | Determine if the organization employs vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities scanned. |  |

### System and Services Acquisition (SA)

|  |  |  |
| --- | --- | --- |
| **SA-1** | **SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES** | **RESULTS** |
| **SA-1.1** | Determine if: |  |
| **SA-1.1.1** | 1. the organization develops and formally documents system and services acquisition policy; |  |
| **SA-1.1.2** | 1. the organization system and services acquisition policy addresses:  * purpose; * scope; * roles and responsibilities; * management commitment; * coordination among organizational entities; and * compliance; |  |
| **SA-1.1.3** | 1. the organization disseminates formal documented system and services acquisition policy to elements within the organization having associated system and services acquisition roles and responsibilities; |  |
| **SA-1.1.4** | 1. the organization develops and formally documents system and services acquisition procedures; |  |
| **SA-1.1.5** | 1. the organization system and services acquisition procedures facilitate implementation of the system and services acquisition policy and associated system and services acquisition controls; and |  |
| **SA-1.1.6** | 1. the organization disseminates formal documented system and services acquisition procedures to elements within the organization having associated system and services acquisition roles and responsibilities. |  |
| **SA-1.2** | Determine if: |  |
| **SA-1.2.1** | 1. the organization defines the frequency of system and services acquisition policy reviews/updates; |  |
| **SA-1.2.2** | 1. the organization reviews/updates system and services acquisition policy in accordance with organization-defined frequency; and |  |
| **SA-1.2.3** | 1. the organization defines the frequency of system and services acquisition procedure reviews/updates; |  |
| **SA-1.2.4** | 1. the organization reviews/updates system and services acquisition procedures in accordance with organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **SA-2** | **ALLOCATION OF RESOURCES** | **RESULTS** |
| **SA-2.1** | Determine if: |  |
| **SA-2.1.1** | 1. the organization determines, documents, and allocates as part of its capital planning and investment control process, the resources required to adequately protect the information system by verifying that the organization:   - defines security requirements for the information system in mission/business   planning;  - establishes a discrete line item for information system security in the   organization’s programming and budgeting documentation; and  - integrates information system security into the capital planning and investment   control process in accordance with the guidance in NIST Special Publication 800-   65. |  |

|  |  |  |
| --- | --- | --- |
| **SA-3** | **LIFE CYCLE SUPPORT** | **RESULTS** |
| **SA-3.1** | Determine if: |  |
| **SA-3.1.1** | 1. the organization manages the information system using a system development life cycle methodology that includes information security considerations; and |  |
| **SA-3.1.2** | 1. the organization uses a system development life cycle that is consistent with NIST Special Publication 800-64. |  |

|  |  |  |
| --- | --- | --- |
| **SA-4** | **ACQUISITIONS** | **RESULTS** |
| **SA-4.1** | Determine if: |  |
| **SA-4.1.1** | 1. the organization includes in acquisition contracts for information systems, either explicitly or by reference, security requirements and/or security specifications based on an assessment of risk and in accordance with applicable laws, Executive Orders, directives, policies, regulations, and standards that describe required:  * security capabilities; * design and development processes; * test and evaluation procedures; and * documentation. |  |
| **SA-4.2.1** | 1. the organization includes in acquisition contracts, requirements for information system documentation addressing user and systems administrator guidance and information regarding the implementation of the security controls in the system and at a level of detail based on the FIPS 199 security category for the system.; and |  |
| **SA-4.3.1** | 1. the organization includes in acquisition contracts requirements for information system documentation that includes security configuration settings and security implementation guidance. |  |

|  |  |  |
| --- | --- | --- |
| **SA-4(1)** | **ACQUISITIONS – CONTROL ENHANCEMENT** | **RESULTS** |
| **SA-4(1).1** | Determine if the organization requires in solicitation documents that appropriate documentation be provided describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls. |  |

|  |  |  |
| --- | --- | --- |
| **SA-4(4)** | **ACQUISITIONS – CONTROL ENHANCEMENT** | **RESULTS** |
| **SA-4(4).1** | Determine if the organization ensures that each information system component acquired is explicitly assigned to an information system, and that the owner of the system acknowledges this assignment. |  |

|  |  |  |
| --- | --- | --- |
| **SA-5** | **INFORMATION SYSTEM DOCUMENTATION** | **RESULTS** |
| **SA-5.1** | Determine if: |  |
| **SA-5.1.1** | 1. the organization obtains, protects as required, and makes available to authorized personnel, information system administrator and user guidance with information on:  * configuring, installing, and operating the information system; and * effectively using the system’s security features; or |  |
| **SA-5.1.2** | 1. the organization, when this information is either unavailable or nonexistent (e.g., due to the age of the system or lack of support from the vendor/manufacturer), the organization documents attempts to obtain such documentation and provides compensating security controls, if needed. |  |

|  |  |  |
| --- | --- | --- |
| **SA-5(1)** | **INFORMATION SYSTEM DOCUMENTATION – CONTROL ENHANCEMENT** | **RESULTS** |
| **SA-5(1).1** | Determine if: |  |
| **SA-5(1).1.1** | 1. the organization includes, in addition to administrator and user guides, documentation, if available from the vendor/manufacturer, describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls. |  |

|  |  |  |
| --- | --- | --- |
| **SA-5(3)** | **INFORMATION SYSTEM DOCUMENTATION – CONTROL ENHANCEMENT** | **RESULTS** |
| **SA-5(3).1** | Determine if the organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the high-level design of the information system in terms of subsystems and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing. |  |

|  |  |  |
| --- | --- | --- |
| **SA-6** | **SOFTWARE USAGE RESTRICTIONS** | **RESULTS** |
| **SA-6.1** | Determine if: |  |
| **SA-6.1.1** | 1. the organization complies with software usage restrictions; and |  |
| **SA-6.1.2** | 1. the organization employs tracking systems to control copying and distribution of software and associated documentation protected by quantity licenses; and |  |
| **SA-6.1.3** | 1. the organization controls and documents the use of publicly accessible 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. |  |

|  |  |  |
| --- | --- | --- |
| **SA-7** | **USER INSTALLED SOFTWARE** | **RESULTS** |
| **SA-7.1** | Determine if the organization enforces explicit rules governing the installation of software by users that include organization-identified types of software installations that are permitted and types of installations that are prohibited. |  |

|  |  |  |
| --- | --- | --- |
| **SA-8** | **SECURITY ENGINEERING PRINCIPLES** | **RESULTS** |
| **SA-8.1** | Determine if: |  |
| **SA-8.1.1** | 1. the organization designs and implements the information system using security engineering principles; and |  |
| **SA-8.1.2** | 1. the organization considers the security design principles in NIST Special Publication 800-27 in the design, development, and implementation of the information system. |  |

|  |  |  |
| --- | --- | --- |
| **SA-9** | **EXTERNAL INFORMATION SYSTEM SERVICES** | **RESULTS** |
| **SA-9.1** | Determine if: |  |
| **SA-9.1.1** | 1. the organization requires that providers of external information system services employ adequate security controls in accordance with applicable laws, Executive Orders, directive, policies, regulations, standards, guidance, and established service-level agreements; and |  |
| **SA-9.1.2** | 1. the organization monitors security control compliance. |  |

|  |  |  |
| --- | --- | --- |
| **SA-10** | **DEVELOPER CONFIGURATION MANAGEMENT** | **RESULTS** |
| **SA-10.1** | Determine if the organization requires that information system developers/integrators: |  |
| **SA-10.1.1** | 1. Perform configuration management during information system design, development, implementation, and operation; |  |
| **SA-10.1.2** | 1. Manage and control changes to the information system; |  |
| **SA-10.1.3** | 1. Implement only organization-approved changes; |  |
| **SA-10.1.4** | 1. Document approved changes to the information system; and |  |
| **SA-10.1.5** | 1. Track security flaws and flaw resolution. |  |

|  |  |  |
| --- | --- | --- |
| **SA-11** | **DEVELOPER SECURITY TESTING** | **RESULTS** |
| **SA-11.1** | Determine if the organization requires that information system developers (and systems integrators) create a security test and evaluation plan, implement the plan, and document the results. |  |

### System and Communication Protection (SC)

|  |  |  |
| --- | --- | --- |
| **SC-1** | **SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES** | **RESULTS** |
| **SC-1.1** | Determine if: |  |
| **SC-1.1.1** | 1. the organization develops and formally documents system and communications protection policy; |  |
| **SC-1.1.2** | 1. the organization system and communications protection policy addresses:  * purpose; * scope; * roles and responsibilities; * management commitment; * coordination among organizational entities; and * compliance; |  |
| **SC-1.1.3** | 1. the organization disseminates formal documented system and communications protection policy to elements within the organization having associated system and communications protection roles and responsibilities; |  |
| **SC-1.1.4** | 1. the organization develops and formally documents system and communications protection procedures; |  |
| **SC-1.1.5** | 1. the organization system and communications protection procedures facilitate implementation of the system and communications protection policy and associated system and communications protection controls; and |  |
| **SC-1.1.6** | 1. the organization disseminates formal documented system and communications protection procedures to elements within the organization having associated system and communications protection roles and responsibilities. |  |
| **SC-1.2** | Determine if: |  |
| **SC-1.2.1** | 1. the organization defines the frequency of system and communications protection policy reviews/updates; |  |
| **SC-1.2.2** | 1. the organization reviews/updates system and communications protection policy in accordance with organization-defined frequency; and |  |
| **SC-1.2.3** | 1. the organization defines the frequency of system and communications protection procedure reviews/updates; |  |
| **SC-1.2.4** | 1. the organization reviews/updates system and communications protection procedures in accordance with organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **SC-2** | **APPLICATION PARTITIONING** | **RESULTS** |
| **SC-2.1** | Determine if: |  |
| **SC-2.1.1** | 1. the information system separates user functionality (including user interface services) from information system management functionality. |  |

|  |  |  |
| --- | --- | --- |
| **SC-4** | **INFORMATION IN SHARED RESOURCES** | **RESULTS** |
| **SC-4.1** | Determine if the information system prevents unauthorized and unintended information transfer via shared system resources. |  |

|  |  |  |
| --- | --- | --- |
| **SC-5** | **DENIAL OF SERVICE PROTECTION** | **RESULTS** |
| **SC-5.1** | Determine if: |  |
| **SC-5.1.1** | 1. the organization defines in the security plan, explicitly or by reference, the types of denial of service attacks (or provides references to sources of current denial of service attacks) that can be addressed by the information system; and |  |
| **SC-5.1.2** | 1. the information system protects against or limits the effects of the organization-defined or referenced types of denial of service attacks. |  |

|  |  |  |
| --- | --- | --- |
| **SC-7** | **BOUNDARY PROTECTION** | **RESULTS** |
| **SC-7.1** | Determine if: |  |
| **SC-7.1.1** | 1. the organization defines key internal boundaries of the information system; and |  |
| **SC-7.2.1** | 1. the information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system. |  |

|  |  |  |
| --- | --- | --- |
| **SC-7(1)** | **BOUNDARY PROTECTION – CONTROL ENHANCEMENT** | **RESULTS** |
| **SC-7(1).1** | Determine if the organization physically allocates publicly accessible information system components to separate subnetworks with separate, physical network interfaces. |  |

|  |  |  |
| --- | --- | --- |
| **SC-7(2)** | **BOUNDARY PROTECTION – CONTROL ENHANCEMENT** | **RESULTS** |
| **SC-7(2).1** | Determine if: |  |
| **SC-7(2).1.1** | 1. the organization defines the mediation necessary for public access to the organization’s internal networks; and |  |
| **SC-7(2).2.1** | 1. the organization prevents public access into the organization’s internal networks except as appropriately mediated. |  |

|  |  |  |
| --- | --- | --- |
| **SC-7(3)** | **BOUNDARY PROTECTION – CONTROL ENHANCEMENT** | **RESULTS** |
| **SC-7(3).1** | Determine if the organization limits the number of access points to the information system to allow for better monitoring of inbound and outbound network traffic. |  |

|  |  |  |
| --- | --- | --- |
| **SC-7(4)** | **BOUNDARY PROTECTION – CONTROL ENHANCEMENT** | **RESULTS** |
| **SC-7(4).1** | Determine if the organization implements a managed interface (boundary protection devices in effective security architecture) with any external telecommunication service, implementing controls appropriate to the required protection of the confidentiality and integrity of the information being transmitted. |  |

|  |  |  |
| --- | --- | --- |
| **SC-7(5)** | **BOUNDARY PROTECTION – CONTROL ENHANCEMENT** | **RESULTS** |
| **SC-7(5).1** | Determine if the information system denies network traffic by default and allows network traffic by exception. |  |

|  |  |  |
| --- | --- | --- |
| **SC-7(7)** | **BOUNDARY PROTECTION – CONTROL ENHANCEMENT** | **RESULTS** |
| **SC-7(7).1** | Determine if the information system prevents remote devices that have established a non-remote connection with the system from communicating outside of that communications path with resources in external networks. |  |

|  |  |  |
| --- | --- | --- |
| **SC-8** | **TRANSMISSION INTEGRITY** | **RESULTS** |
| **SC-8.1** | Determine if the information system protects the integrity of transmitted information. |  |

|  |  |  |
| --- | --- | --- |
| **SC-8(1)** | **BOUNDARY PROTECTION – CONTROL ENHANCEMENT** | **RESULTS** |
| **SC-8(1).1** | Determine if the organization employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures. |  |

|  |  |  |
| --- | --- | --- |
| **SC-9** | **TRANSMISSION CONFIDENTIALITY** | **RESULTS** |
| **SC-9.1** | Determine if the information system protects the confidentiality of transmitted information. |  |

|  |  |  |
| --- | --- | --- |
| **SC-9(1)** | **BOUNDARY PROTECTION – CONTROL ENHANCEMENT** | **RESULTS** |
| **SC-9(1).1** | Determine if organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures. |  |

|  |  |  |
| --- | --- | --- |
| **SC-10** | **NETWORK DISCONNECT** | **RESULTS** |
| **SC-10.1** | Determine if: |  |
| **SC-10.1.1** | 1. the organization defines in the security plan, explicitly or by reference, the time period of inactivity before the information system terminates a network connection; and |  |
| **SC-10.2.1** | 1. the information system terminates a network connection at the end of a session or after the organization-defined time period of inactivity. |  |

|  |  |  |
| --- | --- | --- |
| **SC-12** | **CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT** | **RESULTS** |
| **SC-12.1** | Determine if the organization establishes and manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures, when cryptography is required and employed within the information system. |  |

|  |  |  |
| --- | --- | --- |
| **SC-13** | **USE OF CRYPTOGRAPHY** | **RESULTS** |
| **SC-13.1** | Determine if for information requiring cryptographic protection, the information system implements cryptographic mechanisms that comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. |  |

|  |  |  |
| --- | --- | --- |
| **SC-14** | **PUBLIC ACCESS PROTECTIONS** | **RESULTS** |
| **SC-14.1** | Determine if the information system protects the integrity and availability of publicly available information and applications. |  |

|  |  |  |
| --- | --- | --- |
| **SC-15** | **COLLABORATIVE COMPUTING** | **RESULTS** |
| **SC-15.1** | Determine if the information system prohibits remote activation of collaborative computing mechanisms and provides an explicit indication of use to the local users. |  |

|  |  |  |
| --- | --- | --- |
| **SC-17** | **PUBLIC KEY INFRASTRUCTURE CERTIFICATES** | **RESULTS** |
| **SC-17.1** | Determine if the organization issues public key certificates under an appropriate certificates policy or obtains public key certificates under an appropriate certificate policy from an approved service provider. |  |

|  |  |  |
| --- | --- | --- |
| **SC-18** | **MOBILE CODE** | **RESULTS** |
| **SC-18.1** | Determine if: |  |
| **SC-18.1.1** | 1. the organization establishes usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously; and |  |
| **SC-18.2.1** | 1. the organization authorizes, monitors, and controls the use of mobile code within the information system. |  |

|  |  |  |
| --- | --- | --- |
| **SC-19** | **VOICE OVER INTERNET PROTOCOL** | **RESULTS** |
| **SC-19.1** | Determine if: |  |
| **SC-19.1.1** | 1. the organization establishes usage restrictions and implementation guidance for Voice over Internet Protocol technologies based on the potential to cause damage to the information system if used maliciously; and |  |
| **SC-19.2.1** | 1. the organization authorizes, monitors, and controls the use of VoIP within the information system. |  |

|  |  |  |
| --- | --- | --- |
| **SC-20** | **SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)** | **RESULTS** |
| **SC-20.1** | Determine if the information system, (if the system provides a name/address resolution service), provides artifacts for additional data origin with authentication and data integrity artifacts along with the authoritative data it returns in response to resolution queries. |  |

|  |  |  |
| --- | --- | --- |
| **SC-22** | **ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE** | **RESULTS** |
| **SC-22.1** | Determine if the information systems that collectively provide name/address resolution service for an organization are fault tolerant and implement role separation. |  |

|  |  |  |
| --- | --- | --- |
| **SC-23** | **SESSION AUTHENTICITY** | **RESULTS** |
| **SC-23.1** | Determine if the information system provides mechanisms to protect the authenticity of communications sessions. |  |

|  |  |  |
| --- | --- | --- |
| **SC-28** | **PROTECTION OF INFORMATION AT REST** | **RESULTS** |
| **SC-28.1** | Determine if the information system protects the confidentiality and integrity of information at rest. |  |

|  |  |  |
| --- | --- | --- |
| **SC-32** | **INFORMATION SYSTEM PARTITIONING** | **RESULTS** |
| **SC-32.1** | Determine if the organization partitions the information system into components residing in separate physical domains (or environments) as deemed necessary. |  |

### System and Information Integrity (SI)

|  |  |  |
| --- | --- | --- |
| **SI-1** | **SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES** | **RESULTS** |
| **SI-1.1** | Determine if: |  |
| **SI-1.1.1** | 1. the organization develops and formally documents system and information integrity policy; |  |
| **SI-1.1.2** | 1. the organization system and information integrity policy addresses:  * purpose; * scope; * roles and responsibilities; * management commitment; * coordination among organizational entities; and * compliance; |  |
| **SI-1.1.3** | 1. the organization disseminates formal documented system and information integrity policy to elements within the organization having associated system and information integrity roles and responsibilities; |  |
| **SI-1.1.4** | 1. the organization develops and formally documents system and information integrity procedures; |  |
| **SI-1.1.5** | 1. the organization system and information integrity procedures facilitate implementation of the system and information integrity policy and associated system and information integrity controls; and |  |
| **SI-1.1.6** | 1. the organization disseminates formal documented system and information integrity procedures to elements within the organization having associated system and information integrity roles and responsibilities. |  |
| **SI-1.2** | Determine if: |  |
| **SI-1.2.1** | 1. the organization defines the frequency of system and information integrity policy reviews/updates; |  |
| **SI-1.2.2** | 1. the organization reviews/updates system and information integrity policy in accordance with organization-defined frequency; and |  |
| **SI-1.2.3** | 1. the organization defines the frequency of system and information integrity procedure reviews/updates; |  |
| **SI-1.2.4** | 1. the organization reviews/updates system and information integrity procedures in accordance with organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **SI-2** | **FLAW REMEDIATION** | **RESULTS** |
| **SI-2.1** | Determine if: |  |
| **SI-2.1.1** | 1. the organization identifies, reports, and corrects information system flaws; |  |
| **SI-2.1.2** | 1. the organization installs newly released security patches, service packs, and hot fixes on the information system in a reasonable timeframe in accordance with organizational policy and procedures; |  |
| **SI-2.1.3** | 1. the organization addresses flaws discovered during security assessments, continuous monitoring, or incident response activities in an expeditious manner in accordance with organizational policy and procedures; |  |
| **SI-2.1.4** | 1. the organization tests information system patches, service packs, and hot fixes for effectiveness and potential side effects before installation; and |  |
| **SI-2.1.5** | 1. the organization captures all appropriate information pertaining to the discovered flaws in the information system, including the cause of the flaws, mitigation activities, and lessons learned. |  |

|  |  |  |
| --- | --- | --- |
| **SI-2(2)** | **FLAW REMEDIATION – CONTROL ENHANCEMENT** | **RESULTS** |
| **SI-2(2).1** | Determine if the organization employs automated mechanisms to periodically and upon demand determine the state of information system components with regard to flaw remediation. |  |

|  |  |  |
| --- | --- | --- |
| **SI-3** | **MALICIOUS CODE PROTECTION** | **RESULTS** |
| **SI-3.1** | Determine if the information system implements malicious code protection by verifying that:   * the organization employs malicious code protection mechanisms at critical information system entry and exit points, and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code; * the malicious code protection mechanisms detect and eradicate malicious code transported by electronic mail, electronic mail attachments, Internet access, removable media, or other common means, or by exploiting information system vulnerabilities; * the organization updates malicious code protection mechanisms whenever new releases are available, to include the latest malicious code definitions, in accordance with organizational configuration management policy and procedures; * the organization considered use of malicious code protection software products from multiple vendors; and * the organization considers the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system. |  |

|  |  |  |
| --- | --- | --- |
| **SI-3(1)** | **MALICIOUS CODE PROTECTION – CONTROL ENHANCEMENT** | **RESULTS** |
| **SI-3(1).1** | Determine if the organization centrally manages malicious code protection mechanisms. |  |

|  |  |  |
| --- | --- | --- |
| **SI-3(2)** | **MALICIOUS CODE PROTECTION – CONTROL ENHANCEMENT** | **RESULTS** |
| **SI-3(2).1** | Determine if the organization automatically updates malicious code protection mechanisms. |  |

|  |  |  |
| --- | --- | --- |
| **SI-3(3)** | **MALICIOUS CODE PROTECTION – CONTROL ENHANCEMENT** | **RESULTS** |
| **SI-3(3).1** | Determine if the information system prevents non-privileged users from circumventing malicious code protection capabilities. |  |

|  |  |  |
| --- | --- | --- |
| **SI-4** | **INFORMATION SYSTEM MONITORING** | **RESULTS** |
| **SI-4.1** | Determine if: |  |
| **SI-4.1.1** | 1. the organization employs tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system; |  |
| **SI-4.1.2** | 1. the organization deploys monitoring devices strategically within the information system (e.g., at selected perimeter locations, near server farms supporting critical applications) to collect essential information; |  |
| **SI-4.1.3** | 1. the organization deploys monitoring devices at ad hoc locations within the information system to track specific transactions; |  |
| **SI-4.1.4** | 1. the organization uses the monitoring devices to track the impact of security changes to the information system; |  |
| **SI-4.1.5** | 1. the organization determines the granularity of the information collected based upon it’s monitoring objectives and the capability of the information system to support such activities; |  |
| **SI-4.1.6** | 1. the organization consults appropriate legal counsel with regard to all information system monitoring activities; and |  |
| **SI-4.1.7** | 1. the organization heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation, based on law enforcement information, intelligence information, or other credible sources of information. |  |

|  |  |  |
| --- | --- | --- |
| **SI-4(2)** | **INFORMATION SYSTEM MONITORING – CONTROL ENHANCEMENT** | **RESULTS** |
| **SI-4(2).1** | Determine if the organization employs automated tools to support near real-time analysis of events. |  |

|  |  |  |
| --- | --- | --- |
| **SI-4(4)** | **INFORMATION SYSTEM MONITORING – CONTROL ENHANCEMENT** | **RESULTS** |
| **SI-4(4).1** | Determine if information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions. |  |

|  |  |  |
| --- | --- | --- |
| **SI-4(5)** | **INFORMATION SYSTEM MONITORING – CONTROL ENHANCEMENT** | **RESULTS** |
| **SI-4(5).1** | Determine if the information system provides near real-time alerts when the following indications of compromise or potential compromise occur:[See audit logging process documentation] |  |

|  |  |  |
| --- | --- | --- |
| **SI-4(6)** | **INFORMATION SYSTEM MONITORING – CONTROL ENHANCEMENT** | **RESULTS** |
| **SI-4(6).1** | Determine if the information system prevents non-privileged users from circumventing intrusion detection and prevention capabilities. |  |

|  |  |  |
| --- | --- | --- |
| **SI-5** | **SECURITY ALERTS AND ADVISORIES** | **RESULTS** |
| **SI-5.1** | Determine if: |  |
| **SI-5.1.1** | 1. the organization receives information system security alerts/advisories on a regular basis; |  |
| **SI-5.2.1** | 1. the organization issues security alerts/advisories to appropriate organizational personnel; |  |
| **SI-5.3.1** | 1. the organization takes appropriate actions in response to security alerts/advisories; and |  |
| **SI-5.4.1** | 1. the organization maintains contact with special interest groups (e.g., information security forums) that:  * facilitate sharing of security-related information (e.g., threats, vulnerabilities, and latest security technologies); * provide access to advice from security professionals; and * improve knowledge of security best practices. |  |

|  |  |  |
| --- | --- | --- |
| **SI-7** | **SOFTWARE AND INFORMATION INTEGRITY** | **RESULTS** |
| **SI-7.1** | Determine if the information system detects unauthorized changes to software and information. |  |

|  |  |  |
| --- | --- | --- |
| **SI-7(1)** | **SOFTWARE AND INFORMATION INTEGRITY – CONTROL ENHANCEMENT** | **RESULTS** |
| **SI-7(1).1** | Determine if the organization reassesses the integrity of software and information by performing weekly checks. |  |

|  |  |  |
| --- | --- | --- |
| **SI-8** | **SPAM PROTECTION** | **RESULTS** |
| **SI-8.1** | Determine if the information system implements spam protection by verifying that the organization:   * employs spam protection mechanisms at critical information system entry points and at workstations, servers, or mobile computing devices on the network; and * employs spam protection mechanisms to detect and take appropriate action on unsolicited message transported by electronic mail, electronic mail attachments, Internet accesses, or other common means. |  |

|  |  |  |
| --- | --- | --- |
| **SI-9** | **INFORMATION INPUT RESTRICTIONS** | **RESULTS** |
| **SI-9.1** | Determine if the organization restricts the capability to input information to the information system to authorized personnel. |  |

|  |  |  |
| --- | --- | --- |
| **SI-10** | **INFORMATION INPUT VALIDATION** | **RESULTS** |
| **SI-10.1** | Determine if the information system checks information for accuracy, completeness, validity, and authenticity by verifying that the system:   * checks for accuracy, completeness, validity, and authenticity of information is accomplished as close to the point of origin as possible; * employs rules to check the valid syntax of information inputs to verify that inputs match specified definitions for format and content; * prescreens information inputs passed to interpreters to prevent the content from being unintentionally interpreted as commands; and * checks the accuracy, completeness, validity, and authenticity of information to the extent guided by organizational policy and operational requirements. |  |

|  |  |  |
| --- | --- | --- |
| **SI-11** | **ERROR HANDLING** | **RESULTS** |
| **SI-11.1** | Determine if: |  |
| **SI-11.1.1** | 1. the information system identifies and handles error conditions in an expeditious manner without providing information that could be exploited by adversaries; |  |
| **SI-11.2.1** | 1. the information system reveals error messages only to authorized individuals; and |  |
| **SI-11.3.1** | 1. the information system does not include sensitive information in error logs or associated administrative messages. |  |

|  |  |  |
| --- | --- | --- |
| **SI-12** | **INFORMATION OUTPUT HANDLING AND RETENTION** | **RESULTS** |
| **SI-12.1** | Determine if: |  |
| **SI-12.1.1** | 1. the organization handles output from the information system in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and operational requirements; and |  |
| **SI-12.2.1** | 1. the organization retains output from the information system in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. |  |

### Information Security Program Management (PM)

|  |  |  |
| --- | --- | --- |
| **PM-1** | **INFORMATION SECURITY PROGRAM PLAN** | **RESULTS** |
| **PM-1.1** | Determine if: |  |
| **PM-1.1.1** | 1. the organization develops an information security program plan for the organization   that:   * provides an overview of the requirements for the security program; * provides a description of the security program management controls and   common controls in place or planned for meeting security program  requirements;   * provides sufficient information about the program management controls and   common controls (including specification of parameters for any assignment and selection operations either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan and a determination of the risk to be incurred if the plan is implemented as intended;   * includes roles, responsibilities, management commitment, coordination among organizational entities, and compliance; * is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations and the Nation; |  |
| **PM-1.1.2** | 1. Reviews the organization-wide information security program plan ***annually***; and |  |
| **PM-1.1.3** | 1. Revises the plan to address organizational changes and problems identified during plan implementation or security control assessments. |  |

|  |  |  |
| --- | --- | --- |
| **PM-2** | **SENIOR INFORMATION SECURITY OFFICER** | **RESULTS** |
| **PM-2.1** | Determine if: |  |
| **PM-2.1.1** | 1. organization appoints a senior information security officer to coordinate, develop, implement, and maintain an organization-wide information security program; and |  |
| **PM-2.1.2** | 1. the organization empowers the senior information security officer with the mission and resources required to coordinate, develop, implement, and maintain an organization-wide information security program. |  |

|  |  |  |
| --- | --- | --- |
| **PM-3** | **INFORMATION SECURITY RESOURCES** | **RESULTS** |
| **PM-3.1** | Determine if: |  |
| **PM-3.1.1** | 1. the organization includes in its capital planning and investment requests the resources needed to implement the information security program; |  |
| **PM-3.1.2** | 1. the organization documents all exceptions to the requirement that all capital planning and investment requests include the resources needed to implement the information security program; |  |
| **PM-3.1.3** | 1. the organization employs a business case/Exhibit 300/Exhibit 53 to record the resources required; and |  |
| **PM-3.1.4** | 1. the organization makes the required information security resources available for expenditure as planned. |  |

|  |  |  |
| --- | --- | --- |
| **PM-4** | **PLAN OF ACTION AND MILESTONES PROCESS** | **RESULTS** |
| **PM-4.1** | Determine if: |  |
| **PM-4.1.1** | 1. the organization implements a process to maintain plans of action and milestones for the security program and the associated organizational information systems; and |  |
| **PM-4.1.2** | 1. the organization implements a process to document the remedial information security actions that mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation. |  |

|  |  |  |
| --- | --- | --- |
| **PM-5** | **INFORMATION SYSTEM INVENTORY** | **RESULTS** |
| **PM-5.1** | Determine if: |  |
| **PM-5.1.1** | 1. the organization develops an inventory of its information systems; and |  |
| **PM-5.1.2** | 1. the organization maintains an inventory of its information systems. |  |

|  |  |  |
| --- | --- | --- |
| **PM-6** | **INFORMATION SECURITY MEASURES OF PERFORMANCE** | **RESULTS** |
| **PM-6.1** | Determine if: |  |
| **PM-6.1.1** | 1. the organization develops information security measures of performance; |  |
| **PM-6.1.2** | 1. the organization monitors information security measures of performance; and |  |
| **PM-6.1.3** | 1. the organization reports on the results of information security measures of performance. |  |

|  |  |  |
| --- | --- | --- |
| **PM-7** | **ENTERPRISE ARCHITECTURE** | **RESULTS** |
| **PM-7.1** | Determine if the organization develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation. |  |

|  |  |  |
| --- | --- | --- |
| **PM-8** | **CRITICAL INFRASTRUCTURE PLAN** | **RESULTS** |
| **PM-8.1** | Determine if: |  |
| **PM-8.1.1** | 1. the organization develops and documents a critical infrastructure and key resource protection plan; |  |
| **PM-8.1.2** | 1. the organization updates the critical infrastructure and key resource protection plan; and |  |
| **PM-8.1.3** | 1. the organization addresses information security issues in the critical infrastructure and key resource protection plan. |  |

|  |  |  |
| --- | --- | --- |
| **PM-9** | **RISK MANAGEMENT STRATEGY** | **RESULTS** |
| **PM-9.1** | Determine if: |  |
| **PM-9.1.1** | 1. the organization develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems; and |  |
| **PM-9.1.2** | 1. the organization implements that strategy consistently across the organization. |  |

|  |  |  |
| --- | --- | --- |
| **PM-10** | **SECURITY AUTHORIZATION PROCESS** | **RESULTS** |
| **PM-10.1** | Determine if: |  |
| **PM-10.1.1** | 1. the organization manages (i.e., documents, tracks, and reports) the security state of organizational information systems through security authorization processes; |  |
| **PM-10.1.2** | 1. the organization designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and |  |
| **PM-10.1.3** | 1. the organization fully integrates the security authorization processes into an organization-wide risk management program. |  |

|  |  |  |
| --- | --- | --- |
| **PM-11** | **MISSION / BUSINESS PROCESS DEFINITION** | **RESULTS** |
| **PM-11.1** | Determine if: |  |
| **PM-11.1.1** | 1. the organization defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and |  |
| **PM-11.1.2** | 1. the organization determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until an achievable set of protection needs is obtained. |  |