INFORMATION ASSURANCE MINIMUM SECURITY CONTROL CHECKLIST

COMMERCIAL SATELLITE COMMUNICATIONS SOLUTIONS (COMSATCOM)

SIN 517410

INSTRUCTIONS:

(i) Federal policy (OMB Circular A-130) specifies Government customer compliance with the Federal Information Security Modernization Act of 2014 (FISMA 2014) as implemented by Federal Information Processing Standards Publication 200 (FIPS 200), *Minimum Security Requirements for Federal Information and Information Systems*. This standard specifies minimum security requirements Federal agencies and federal contractors must meet, defined through the use of security controls described in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev. 5, “*Security and Privacy Controls for Information Systems and Organizations*.”

(ii) Complete the enclosed Information Assurance Checklist. The purpose of Control Implementation Statements is to provide an overview of the intended application of each selected control in the context of a specific system with a sufficient level of detail to correctly implement the control and to subsequently assess the effectiveness of the control as implemented in the system. For Organizational Defined Parameters (ODP) in *[brackets]* found within some of the descriptions, please replace the *[brackets]* with information about how you currently execute or propose to implement those items.

(iii) The Government will evaluate the Information Assurance Checklist submitted as part of Offeror’s proposal to determine whether the Offeror understands the minimum security controls, and has processes, personnel, and infrastructure that currently complies or demonstrates a reasonable approach to becoming compliant with all the minimum security controls for at least a low-impact information system. Text for the low-impact information system controls are included in the table.

Additional security controls may be determined at the task-order level. The tables below note controls which may be applicable for Moderate or High Impact systems. The tables below also include a mapping to the United States Space Force (USSF) Commercial Satellite Communications Office (CSCO) Infrastructure Asset Pre-Assessment (IA-Pre) Security Controls List. The USSF CSCO is the program office that oversees the procurement of all COMSATCOM for the DoD and is by far our largest customer. The IA-Pre assessments will be conducted by the USSF for assets owned by COMSATCOM vendors separately from our IA Checklist review process, but we wanted to inform vendors of that process and provide a mapping to the IA-Pre controls list for your reference.

Note: Control Enhancements that are included in IA-PRE but are not part of the minimum security controls are noted in the IA-PRE column corresponding to the parent control.

| **References** | | **CONTROL NAME** | **Threshold Compliance** | | |
| --- | --- | --- | --- | --- | --- |
| **IA-PRE** | **NIST 800-53** | **Low-Impact Information System (FIPS 200 / NIST SP 800-53)  (generally commercial best practices)** | **Explain Your Current Compliance OR Actions to Become Compliant** | **Control Implementation Status** |
|  | | | | |  |
| **Access Control (AC)** | | | | | |
| AC-01 | AC-1 | ACCESS CONTROL POLICY AND PROCEDURES | a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:  1. [Selection (one or more): Organization-level; Mission/business process-level; System level] access control policy that:  (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and  (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and  2. Procedures to facilitate the implementation of the access control policy and the associated access controls;  b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the access control policy and procedures; and  c. Review and update the current access control:  1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and  2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]. |  |  |
| AC-02  AC-02-01  AC-02-02  AC-02-03  AC-02-04  AC-02-05  AC-02-06  AC-02-07  AC-02-08  AC-02-09  AC-02-10  AC-02-11  AC-02-12  AC-02-13 | AC-2 | ACCOUNT MANAGEMENT | a. Define and document the types of accounts allowed and specifically prohibited for use within the system;  b. Assign account managers;  c. Require [Assignment: organization-defined prerequisites and criteria] for group and role membership;  d. Specify:  1. Authorized users of the system;  2. Group and role membership; and  3. Access authorizations (i.e., privileges) and [Assignment: organization-defined attributes (as required)] for each account;  e. Require approvals by [Assignment: organization-defined personnel or roles] for requests to create accounts;  f. Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, prerequisites, and criteria];  g. Monitor the use of accounts;  h. Notify account managers and [Assignment: organization-defined personnel or roles] within:  1. [Assignment: organization-defined time period] when accounts are no longer required;  2. [Assignment: organization-defined time period] when users are terminated or transferred; and  3. [Assignment: organization-defined time period] when system usage or need-to-know changes for an individual;  i. Authorize access to the system based on:  1. A valid access authorization;  2. Intended system usage; and  3. [Assignment: organization-defined attributes (as required)];  j. Review accounts for compliance with account management requirements [Assignment: organization-defined frequency];  k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and  l. Align account management processes with personnel termination and transfer processes |  |  |
| AC-03  AC-03-04 | AC-3 | ACCESS ENFORCEMENT | Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies. |  |  |
| AC-04 | AC-4 | INFORMATION FLOW ENFORCEMENT | Not Applicable for NIST Low-Impact Information Systems | Optional: (May be applicable for NIST Moderate or High Impact) |  |
| AC-05 | AC-5 | SEPARATION OF DUTIES | Not Applicable for NIST Low-Impact Information Systems | Optional: (May be applicable for NIST Moderate or High Impact) |  |
| AC-06  AC-06-01  AC-06-02  AC-06-03  AC-06-05  AC-06-07  AC-06-08  AC-06-09  AC-06-10 | AC-6 | LEAST PRIVILEGE | Not Applicable for NIST Low-Impact Information Systems | Optional: (May be applicable for NIST Moderate or High Impact) |  |
| AC-07 | AC-7 | UNSUCCESSFUL LOGIN ATTEMPTS | a. Enforce a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period]; and  b. Automatically [Selection (one or more): lock the account or node for an [Assignment: organization-defined time period]; lock the account or node until released by an administrator; delay next logon prompt per [Assignment: organization-defined delay algorithm]; notify system administrator; take other [Assignment: organization-defined action]] when the maximum number of unsuccessful attempts is exceeded. |  |  |
| AC-08 | AC-8 | SYSTEM USE NOTIFICATION | a. Display [Assignment: organization-defined system use notification message or banner] to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and state that:  1. Users are accessing a U.S. Government system;  2. System usage may be monitored, recorded, and subject to audit;  3. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and  4. Use of the system indicates consent to monitoring and recording;  b. Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system; and  c. For publicly accessible systems:  1. Display system use information [Assignment: organization-defined conditions], before granting further access to the publicly accessible system;  2. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and  3. Include a description of the authorized uses of the system |  |  |
| AC-10 | AC-10 | CONCURRENT SESSION CONTROL | Not Applicable for NIST Low-Impact Information Systems | Optional: (May be applicable for NIST High Impact) |  |
| AC-11  AC-11-01 | AC-11 | DEVICE LOCK | Not Applicable for NIST Low-Impact Information Systems | Optional: (May be applicable for NIST Moderate or High Impact) |  |
| AC-12  AC-12-01 | AC-12 | SESSION TERMINATION | Withdrawn: Incorporated into SC-10 |  |  |
| AC-14 | AC-14 | PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION | a. Identify [Assignment: organization-defined user actions] that can be performed on the system without identification or authentication consistent with organizational mission and business functions; and  b. Document and provide supporting rationale in the security plan for the system, user actions not requiring identification or authentication. |  |  |
| AC-16  AC-16-06 | AC-16 | SECURITY AND PRIVACY ATTRIBUTES | Not Applicable for NIST Low-Impact Information Systems |  |  |
| AC-17-01  AC-17-02  AC-17-03  AC-17-04  AC-17-06  AC-17-09 | AC-17 | REMOTE ACCESS | a. Identify [Assignment: organization-defined user actions] that can be performed on the system without identification or authentication consistent with organizational mission and business functions; and  b. Document and provide supporting rationale in the security plan for the system, user actions not requiring identification or authentication. |  |  |
| AC-18  AC-18-01  AC-18-03  AC-18-04  AC-18-05 | AC-18 | WIRELESS ACCESS | a. Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access; and  b. Authorize each type of wireless access to the system prior to allowing such connections. |  |  |
| AC-19  AC-19-05 | AC-19 | ACCESS CONTROL FOR MOBILE DEVICES | a. Establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas; and  b. Authorize the connection of mobile devices to organizational systems. |  |  |
| AC-20  AC-20-01  AC-20-02  AC-20-03 | AC-20 | USE OF EXTERNAL INFORMATION SYSTEMS | a. [Selection (one or more): Establish [Assignment: organization-defined terms and conditions]; Identify [Assignment: organization-defined controls asserted to be implemented on external systems]], consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to:  1. Access the system from external systems; and  2. Process, store, or transmit organization-controlled information using external systems; or  b. Prohibit the use of [Assignment: organizationally-defined types of external systems]. |  |  |
| AC-21 | AC-21 | USER-BASED COLLABORATION AND INFORMATION SHARING | Not Applicable for NIST Low-Impact Information Systems |  |  |
| AC-22 | AC-22 | PUBLICLY ACCESSIBLE CONTENT | a. Designate individuals authorized to make information publicly accessible;  b. Train authorized individuals to ensure that publicly accessible information does not contain  nonpublic information;  c. Review the proposed content of information prior to posting onto the publicly accessible system to ensure that nonpublic information is not included; and  d. Review the content on the publicly accessible system for nonpublic information [Assignment: organization-defined frequency] and remove such information, if discovered. |  |  |
| AC-23 | AC-23 | DATA MINING PROTECTION | Not Applicable for NIST Low-Impact Information Systems |  |  |
| **Awareness and Training (AT)** | | | | | |
| AT-01 | AT-1 | POLICY AND PROCEDURES | a. Develop, document, and disseminate to [Assignment: organization-defined personnel or  roles]:  1. [Selection (one or more): Organization-level; Mission/business process-level; System level] awareness and training policy that:  (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and  (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and  2. Procedures to facilitate the implementation of the awareness and training policy and the associated awareness and training controls;  b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the awareness and training policy and procedures; and  c. Review and update the current awareness and training:  1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and  2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]. |  |  |
| AT-02 | AT-2 | LITERACY TRAINING AND AWARENESS | a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors):  1. As part of initial training for new users and [Assignment: organization-defined frequency] thereafter; and  2. When required by system changes or following [Assignment: organization-defined events];  b. Employ the following techniques to increase the security and privacy awareness of system users [Assignment: organization-defined awareness techniques];  c. Update literacy training and awareness content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and  d. Incorporate lessons learned from internal or external security incidents or breaches into literacy training and awareness techniques. |  |  |
| AT-02-02 | AT-2(2) | LITERACY TRAINING AND AWARENESS | INSIDER THREAT | Provide literacy training on recognizing and reporting potential indicators of insider threat. |  |  |
| AT-03  AT-03-02  AT-03-04 | AT-3 | ROLE-BASED TRAINING | a. Provide role-based security and privacy training to personnel with the following roles and responsibilities: [Assignment: organization-defined roles and responsibilities]:  1. Before authorizing access to the system, information, or performing assigned duties, and [Assignment: organization-defined frequency] thereafter; and  2. When required by system changes;  b. Update role-based training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and  c. Incorporate lessons learned from internal or external security incidents or breaches into role-based training. |  |  |
| AT-04 | AT-4 | TRAINING RECORDS | a. Document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training; and  b. Retain individual training records for [Assignment: organization-defined time period]. |  |  |
| **Audit and Accountability (AU)** | | | | | |
| AU-01 | AU-1 | POLICY AND PROCEDURES | a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:  1. [Selection (one or more): Organization-level; Mission/business process-level; System level] audit and accountability policy that:  (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and  (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and  2. Procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls;  b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the audit and accountability policy and procedures; and  c. Review and update the current audit and accountability:  1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and  2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]. |  |  |
| AU-02  AU-02-03 | AU-2 | EVENT LOGGING | a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging];  b. Coordinate the event logging function with other organizational entities requiring audit related information to guide and inform the selection criteria for events to be logged;  c. Specify the following event types for logging within the system: [Assignment: organization defined event types (subset of the event types defined in AU-2a.) along with the frequency of (or situation requiring) logging for each identified event type];  d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and  e. Review and update the event types selected for logging [Assignment: organization-defined frequency]. |  |  |
| AU-03  AU-03-01  AU-03-02 | AU-3 | CONTENT OF AUDIT RECORDS | Ensure that audit records contain information that establishes the following:  a. What type of event occurred;  b. When the event occurred;  c. Where the event occurred;  d. Source of the event;  e. Outcome of the event; and  f. Identity of any individuals, subjects, or objects/entities associated with the event. |  |  |
| AU-04  AU-04-01 | AU-4 | AUDIT LOG STORAGE CAPACITY | Allocate audit log storage capacity to accommodate [Assignment: organization-defined audit log retention requirements]. |  |  |
| AU-05  AU-05-01  AU-05-02 | AU-5 | RESPONSE TO AUDIT LOGGING PROCESS FAILURES | a. Alert [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period] in the event of an audit logging process failure; and  b. Take the following additional actions: [Assignment: organization-defined additional actions]. |  |  |
| AU-06  AU-06-01  AU-06-03  AU-06-04  AU-06-05  AU-06-06  AU-06-10 | AU-6 | AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | a. Review and analyze system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity] and the potential impact of the inappropriate or unusual activity;  b. Report findings to [Assignment: organization-defined personnel or roles]; and  c. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information. |  |  |
| AU-07  AU-07-01 | AU-7 | AUDIT RECORD REDUCTION AND REPORT GENERATION | Not Applicable for NIST Low-Impact Information Systems | Optional: (May be applicable for NIST Moderate or High Impact) |  |
| AU-08  AU-08-01 | AU-8 | TIME STAMPS | a. Use internal system clocks to generate time stamps for audit records; and  b. Record time stamps for audit records that meet [Assignment: organization-defined granularity of time measurement] and that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as  part of the time stamp. |  |  |
| AU-09  AU-09-02  AU-09-03  AU-09-04 | AU-9 | PROTECTION OF AUDIT INFORMATION | a. Protect audit information and audit logging tools from unauthorized access, modification, and deletion; and  b. Alert [Assignment: organization-defined personnel or roles] upon detection of unauthorized access, modification, or deletion of audit information. |  |  |
| AU-10 | AU-10 | NON-REPUDIATION | Not Applicable for NIST Low-Impact Information Systems | Optional: (May be applicable for NIST High Impact) |  |
| AU-11  AU-11-01 | AU-11 | AUDIT RECORD RETENTION | Retain audit records for [Assignment: organization-defined time period consistent with records retention policy] to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements. |  |  |
| AU-12  AU-12-01 AU-12-03 | AU-12 | AUDIT RECORD GENERATION | a. Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2a on [Assignment: organization-defined system components];  b. Allow [Assignment: organization-defined personnel or roles] to select the event types that are to be logged by specific components of the system; and  c. Generate audit records for the event types defined in AU-2c that include the audit record content defined in AU-3. |  |  |
| AU-14  AU-14-01 AU-14-02 AU-14-03 | AU-14 | SESSION AUDIT | Not Applicable for NIST Low-Impact Information Systems |  |  |
| **Assessment, Authorization and Monitoring (CA)** | | | | | |
| CA-01 | CA-1 | POLICIES AND PROCEDURES | a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:  1. [Selection (one or more): Organization-level; Mission/business process-level; System level] assessment, authorization, and monitoring policy that:  (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and  (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and  2. Procedures to facilitate the implementation of the assessment, authorization, and monitoring policy and the associated assessment, authorization, and monitoring controls;  b. Designate an [Assignment: organization-defined official] to manage the development,  documentation, and dissemination of the assessment, authorization, and monitoring policy  and procedures; and  c. Review and update the current assessment, authorization, and monitoring:  1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and  2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]. |  |  |
| CA-02  CA-02-01 CA-02-02 | CA-2 | CONTROL ASSESSMENTS | a. Select the appropriate assessor or assessment team for the type of assessment to be conducted;  b. Develop a control assessment plan that describes the scope of the assessment including:  1. Controls and control enhancements under assessment;  2. Assessment procedures to be used to determine control effectiveness; and  3. Assessment environment, assessment team, and assessment roles and responsibilities;  c. Ensure the control assessment plan is reviewed and approved by the authorizing official or  designated representative prior to conducting the assessment;  d. Assess the controls in the system and its environment of operation [Assignment: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements;  e. Produce a control assessment report that document the results of the assessment; and  f. Provide the results of the control assessment to [Assignment: organization-defined individuals or roles]. |  |  |
| CA-03  CA-03-01  CA-03-05 | CA-3 | INFORMATION EXCHANGE | a. Approve and manage the exchange of information between the system and other systems using [Selection (one or more): interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service level agreements; user agreements; nondisclosure agreements; [Assignment: organization-defined type of agreement]];  b. Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated; and  c. Review and update the agreements [Assignment: organization-defined frequency]. |  |  |
| CA-05 | CA-5 | PLAN OF ACTION AND MILESTONES | a. Develop a plan of action and milestones for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and  b. Update existing plan of action and milestones [Assignment: organization-defined frequency] based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities |  |  |
| CA-06 | CA-6 | AUTHORIZATION | a. Assign a senior official as the authorizing official for the system;  b. Assign a senior official as the authorizing official for common controls available for inheritance by organizational systems;  c. Ensure that the authorizing official for the system, before commencing operations:  1. Accepts the use of common controls inherited by the system; and  2. Authorizes the system to operate;  d. Ensure that the authorizing official for common controls authorizes the use of those controls for inheritance by organizational systems;  e. Update the authorizations [Assignment: organization-defined frequency]. |  |  |
| CA-07  CA-07-01 | CA-7 | CONTINUOUS MONITORING | Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes:  a. Establishing the following system-level metrics to be monitored: [Assignment: organization defined system-level metrics];  b. Establishing [Assignment: organization-defined frequencies] for monitoring and  [Assignment: organization-defined frequencies] for assessment of control effectiveness;  c. Ongoing control assessments in accordance with the continuous monitoring strategy;  d. Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy;  e. Correlation and analysis of information generated by control assessments and monitoring;  f. Response actions to address results of the analysis of control assessment and monitoring information; and  g. Reporting the security and privacy status of the system to [Assignment: organization defined personnel or roles] [Assignment: organization-defined frequency]. |  |  |
| NA | CA-7(4) | CONTINUOUS MONITORING | RISK MONITORING | Ensure risk monitoring is an integral part of the continuous monitoring strategy that includes the following:  (a) Effectiveness monitoring;  (b) Compliance monitoring; and  (c) Change monitoring. |  |  |
| CA-08 | CA-8 | PENETRATION TESTING | Not Applicable for NIST Low-Impact Information Systems | Optional: (May be applicable for NIST High Impact) |  |
| CA-09 | CA-9 | INTERNAL SYSTEM CONNECTIONS | a. Authorize internal connections of [Assignment: organization-defined system components or classes of components] to the system;  b. Document, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated;  c. Terminate internal system connections after [Assignment: organization-defined conditions]; and  d. Review [Assignment: organization-defined frequency] the continued need for each internal connection. |  |  |
| **Configuration Management (CM)** | | | | |  |
| CM-01 | CM-1 | POLICY AND PROCEDURES | a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:  1. [Selection (one or more): Organization-level; Mission/business process-level; System level] configuration management policy that:  (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and  (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and  2. Procedures to facilitate the implementation of the configuration management policy and the associated configuration management controls;  b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the configuration management policy and procedures; and  c. Review and update the current configuration management:  1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and  2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]. |  |  |
| CM-02  CM-02-01  CM-02-02  CM-02-03  CM-02-07 | CM-2 | BASELINE CONFIGURATION | a. Develop, document, and maintain under configuration control, a current baseline configuration of the system; and  b. Review and update the baseline configuration of the system:  1. [Assignment: organization-defined frequency];  2. When required due to [Assignment: organization-defined circumstances]; and  3. When system components are installed or upgraded. |  |  |
| CM-03  CM-03-01  CM-03-02  CM-03-04  CM-03-05  CM-03-06 | CM-3 | CONFIGURATION CHANGE CONTROL | Not Applicable for NIST Low-Impact Information Systems | Optional: (May be applicable for NIST Moderate or High Impact) |  |
| CM-04  CM-04-01 | CM-4 | IMPACT ANALYSIS | Analyze changes to the system to determine potential security and privacy impacts prior to change implementation. |  |  |
| CM-05  CM-05-01  CM-05-02  CM-05-03  CM-05-05  CM-05-06 | CM-5 | ACCESS RESTRICTIONS FOR CHANGE | Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system |  |  |
| CM-06  CM-06-01  CM-06-02 | CM-6 | CONFIGURATION SETTINGS | a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using [Assignment: organization-defined common secure configurations];  b. Implement the configuration settings;  c. Identify, document, and approve any deviations from established configuration settings for [Assignment: organization-defined system components] based on [Assignment: organization defined operational requirements]; and  d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures. |  |  |
| CM-07  CM-07-01  CM-07-02  CM-07-03  CM-07-05 | CM-7 | LEAST FUNCTIONALITY | a. Configure the system to provide only [Assignment: organization-defined mission essential capabilities]; and  b. Prohibit or restrict the use of the following functions, ports, protocols, software, and/or services: [Assignment: organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services]. |  |  |
| CM-08  CM-08-01  CM-08-02  CM-08-03  CM-08-04  CM-08-05 | CM-8 | SYSTEM COMPONENT INVENTORY | a. Develop and document an inventory of system components that:  1. Accurately reflects the system;  2. Includes all components within the system;  3. Does not include duplicate accounting of components or components assigned to any other system;  4. Is at the level of granularity deemed necessary for tracking and reporting; and  5. Includes the following information to achieve system component accountability:[Assignment: organization-defined information deemed necessary to achieve effective system component accountability]; and  b. Review and update the system component inventory [Assignment: organization-defined frequency]. |  |  |
| CM-09 | CM-9 | CONFIGURATION MANAGEMENT PLAN | Not Applicable for NIST Low-Impact Information Systems | Optional: (May be applicable for NIST Moderate or High Impact) |  |
| CM-10  CM-10-01 | CM-10 | SOFTWARE USAGE RESTRICTIONS | a. Use software and associated documentation in accordance with contract agreements and copyright laws;  b. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and  c. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work. |  |  |
| CM-11  CM-11-01  CM-11-02 | CM-11 | USER-INSTALLED SOFTWARE | a. Establish [Assignment: organization-defined policies] governing the installation of software by users;  b. Enforce software installation policies through the following methods: [Assignment: organization-defined methods]; and  c. Monitor policy compliance [Assignment: organization-defined frequency]. |  |  |
| NA | CM-12 | INFORMATION LOCATION | Not Applicable for NIST Low-Impact Information Systems | Optional: (May be applicable for NIST Moderate or High Impact) |  |
| **Contingency Planning (CP)** | | | | | |
| CP-01 | CP-1 | POLICY AND PROCEDURES | a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:  1. [Selection (one or more): Organization-level; Mission/business process-level; System level] contingency planning policy that:  (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and  (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and  2. Procedures to facilitate the implementation of the contingency planning policy and the associated contingency planning controls;  b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the contingency planning policy and procedures; and  c. Review and update the current contingency planning:  1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and  2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]. |  |  |
| CP-02  CP-02-01  CP-02-02  CP-02-03  CP-02-04  CP-02-05  CP-02-08 | CP-2 | CONTINGENCY PLAN | a. Develop a contingency plan for the system that:  1. Identifies essential mission and business functions and associated contingency  requirements;  2. Provides recovery objectives, restoration priorities, and metrics;  3. Addresses contingency roles, responsibilities, assigned individuals with contact information;  4. Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure;  5. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented;  6. Addresses the sharing of contingency information; and  7. Is reviewed and approved by [Assignment: organization-defined personnel or roles];  b. Distribute copies of the contingency plan to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements];  c. Coordinate contingency planning activities with incident handling activities;  d. Review the contingency plan for the system [Assignment: organization-defined frequency];  e. Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;  f. Communicate contingency plan changes to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements];  g. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training; and  h. Protect the contingency plan from unauthorized disclosure and modification. |  |  |
| CP-03  CP-03-01 | CP-3 | CONTINGENCY TRAINING | a. Provide contingency training to system users consistent with assigned roles and responsibilities:  1. Within [Assignment: organization-defined time period] of assuming a contingency role or responsibility;  2. When required by system changes; and  3. [Assignment: organization-defined frequency] thereafter; and  b. Review and update contingency training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]. |  |  |
| CP-04  CP-04-01  CP-04-02 | CP-4 | CONTINGENCY PLAN TESTING | a. Test the contingency plan for the system [Assignment: organization-defined frequency] using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: [Assignment: organization-defined tests].  b. Review the contingency plan test results; and  c. Initiate corrective actions, if needed. |  |  |
| CP-06  CP-06-01 CP-06-02 CP-06-03 | CP-6 | ALTERNATE STORAGE SITE | Not Applicable for NIST Low-Impact Information Systems | May be applicable for NIST Moderate or High Impact) |  |
| CP-07  CP-07-01 CP-07-02  CP-07-03 CP-07-04 | CP-7 | ALTERNATE PROCESSING SITE | Not Applicable for NIST Low-Impact Information Systems | Optional: (May be applicable for NIST Moderate or High Impact) |  |
| CP-08  CP-08-01  CP-08-02  CP-08-03  CP-08-04  CP-08-05 | CP-8 | TELECOMMUNICA­TIONS SERVICES | Not Applicable for NIST Low-Impact Information Systems | Optional: (May be applicable for NIST Moderate or High Impact) |  |
| CP-09  CP-09-01 CP-09-02  CP-09-03 CP-09-05 | CP-9 | SYSTEM BACKUP | a. Conduct backups of user-level information contained in [Assignment: organization-defined system components] [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives];  b. Conduct backups of system-level information contained in the system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives];  c. Conduct backups of system documentation, including security- and privacy-related documentation [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; and  d. Protect the confidentiality, integrity, and availability of backup information. |  |  |
| CP-10  CP-10-02  CP-10-04 | CP-10 | SYSTEM RECOVERY AND RECONSTITUTION | Provide for the recovery and reconstitution of the system to a known state within [Assignment: organization-defined time period consistent with recovery time and recovery point objectives] after a disruption, compromise, or failure. |  |  |
| **Identification and Authentication (IA)** | | | | | |
| IA-01 | IA-1 | POLICY AND PROCEDURES | a. Develop, document, and disseminate to [Assignment: organization-defined personnel or  roles]:  1. [Selection (one or more): Organization-level; Mission/business process-level; System level] identification and authentication policy that:  (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and  (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and  2. Procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls;  b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the identification and authentication policy and procedures; and  c. Review and update the current identification and authentication:  1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and  2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]. |  |  |
| IA-02  IA-02-03  IA-02-04  IA-02-05  IA-02-09  IA-02-11 | IA-2 | IDENTIFICATION AND AUTHENTICATION (Organizational Users) | Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users. |  |  |
| IA-02-01 | IA-2(1) |  | (1) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | MULTI-FACTOR  AUTHENTICATION TO PRIVILEGED ACCOUNTS  Implement multi-factor authentication for access to privileged accounts. |  |  |
| IA-02-02 | IA-2(2) |  | (2) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | MULTI-FACTOR  AUTHENTICATION TO NON-PRIVILEGED ACCOUNTS  Implement multi-factor authentication for access to non-privileged accounts. |  |  |
| IA-02-08 | IA-2(8) |  | (8) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | ACCESS TO ACCOUNTS —  REPLAY RESISTANT  Implement replay-resistant authentication mechanisms for access to [Selection (one or more): privileged accounts; non-privileged accounts]. |  |  |
| IA-02-12 | IA-2(12) |  | Accept and electronically verify Personal Identity Verification-compliant credentials. |  |  |
| IA-03  IA-03-01 | IA-3 | DEVICE IDENTIFICATION AND AUTHENTICATION | Not Applicable for NIST Low-Impact Information Systems | Optional: (May be applicable for NIST Moderate or High Impact) |  |
| IA-04  IA-04-04 | IA-4 | IDENTIFIER MANAGEMENT | Manage system identifiers by:  a. Receiving authorization from [Assignment: organization-defined personnel or roles] to assign an individual, group, role, service, or device identifier;  b. Selecting an identifier that identifies an individual, group, role, service, or device;  c. Assigning the identifier to the intended individual, group, role, service, or device; and  d. Preventing reuse of identifiers for [Assignment: organization-defined time period]. |  |  |
| IA-05  IA-05-02  IA-05-03  IA-05-04  IA-05-07  IA-05-08 IA-05-11  IA-05-13  IA-05-14 | IA-5 | AUTHENTICATOR MANAGEMENT | Manage system authenticators by:  a. Verifying, as part of the initial authenticator distribution, the identity of the individual,  group, role, service, or device receiving the authenticator;  b. Establishing initial authenticator content for any authenticators issued by the organization;  c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;  d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators;  e. Changing default authenticators prior to first use;  f. Changing or refreshing authenticators [Assignment: organization-defined time period by authenticator type] or when [Assignment: organization-defined events] occur;  g. Protecting authenticator content from unauthorized disclosure and modification;  h. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; and  i. Changing authenticators for group or role accounts when membership to those accounts changes. |  |  |
| IA-05-01 | IA-5(1) | AUTHENTICATOR MANAGEMENT | PASSWORD-BASED AUTHENTICATION | For password-based authentication:  (a) Maintain a list of commonly-used, expected, or compromised passwords and update the list [Assignment: organization-defined frequency] and when organizational passwords are suspected to have been compromised directly or indirectly;  (b) Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5(1)(a);  (c) Transmit passwords only over cryptographically-protected channels;  (d) Store passwords using an approved salted key derivation function, preferably using a keyed hash;  (e) Require immediate selection of a new password upon account recovery;  (f) Allow user selection of long passwords and passphrases, including spaces and all printable characters;  (g) Employ automated tools to assist the user in selecting strong password authenticators; and  (h) Enforce the following composition and complexity rules: [Assignment: organization defined composition and complexity rules]. |  |  |
| IA-06 | IA-6 | AUTHENTICATOR FEEDBACK | Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals. |  |  |
| IA-07 | IA-7 | CRYPTOGRAPHIC MODULE AUTHENTICATION | Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication. |  |  |
| IA-08  IA-08-03 | IA-8 | IDENTIFICATION AND AUTHENTICATION (Non-Organizational Users) | Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users. |  |  |
| IA-08-01 | IA-8(1) | IDENTIFICATION AND AUTHENTICATION (NON ORGANIZATIONAL USERS) | ACCEPTANCE OF PIV  CREDENTIALS FROM OTHER AGENCIES | Accept and electronically verify Personal Identity Verification-compliant credentials from other federal agencies. |  |  |
| IA-08-02 | IA-8(2) | IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | ACCEPTANCE OF EXTERNAL  AUTHENTICATORS | (a) Accept only external authenticators that are NIST-compliant; and  (b) Document and maintain a list of accepted external authenticators. |  |  |
| IA-08-04 | IA-8(4) | IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | USE OF DEFINED PROFILES | Conform to the following profiles for identity management [Assignment: organization-defined identity management profiles]. |  |  |
| IA-10 | IA-10 | ADAPTIVE AUTHENTICATION | Not Applicable for NIST Low-Impact Information Systems |  |  |
| IA-11 | IA-11 | RE-AUTHENTICATION | Require users to re-authenticate when [Assignment: organization-defined circumstances or situations requiring re-authentication]. |  |  |
| NA | IA-12 | IDENTITY PROOFING | Not Applicable for NIST Low-Impact Information Systems | Optional: (May be applicable for NIST Moderate or High Impact) |  |
| **Incident Response (IR)** | | | | | |
| IR-01 | IR-1 | POLICY AND PROCEDURES | a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:  1. [Selection (one or more): Organization-level; Mission/business process-level; System level] incident response policy that:  (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and  (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and  2. Procedures to facilitate the implementation of the incident response policy and the associated incident response controls;  b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the incident response policy and procedures; and  c. Review and update the current incident response:  1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and  2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]. |  |  |
| IR-02  IR-02-01  IR-02-02 | IR-2 | INCIDENT RESPONSE TRAINING | a. Provide incident response training to system users consistent with assigned roles and responsibilities:  1. Within [Assignment: organization-defined time period] of assuming an incident response role or responsibility or acquiring system access;  2. When required by system changes; and  3. [Assignment: organization-defined frequency] thereafter; and  b. Review and update incident response training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]. |  |  |
| IR-03  IR-03-02 | IR-3 | INCIDENT RESPONSE TESTING | Not Applicable for NIST Low-Impact Information Systems | Optional: (May be applicable for NIST Moderate or High Impact) |  |
| IR-04  IR-04-01  IR-04-03  IR-04-04  IR-04-06  IR-04-07  IR-04-08 | IR-4 | INCIDENT HANDLING | a. Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery;  b. Coordinate incident handling activities with contingency planning activities;  c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly; and  d. Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization. |  |  |
| IR-05  IR-05-01 | IR-5 | INCIDENT MONITORING | Track and document incidents. |  |  |
| IR-06  IR-06-01  IR-06-02 | IR-6 | INCIDENT REPORTING | a. Require personnel to report suspected incidents to the organizational incident response capability within [Assignment: organization-defined time period]; and  b. Report incident information to [Assignment: organization-defined authorities]. |  |  |
| IR-07  IR-07-01  IR-07-02 | IR-7 | INCIDENT RESPONSE ASSISTANCE | Provide an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the system for the handling and reporting of incidents. |  |  |
| IR-08 | IR-8 | INCIDENT RESPONSE PLAN | a. Develop an incident response plan that:  1. Provides the organization with a roadmap for implementing its incident response capability;  2. Describes the structure and organization of the incident response capability;  3. Provides a high-level approach for how the incident response capability fits into the overall organization;  4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;  5. Defines reportable incidents;  6. Provides metrics for measuring the incident response capability within the organization;  7. Defines the resources and management support needed to effectively maintain and mature an incident response capability;  8. Addresses the sharing of incident information;  9. Is reviewed and approved by [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency]; and  10. Explicitly designates responsibility for incident response to [Assignment: organization defined entities, personnel, or roles].  b. Distribute copies of the incident response plan to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements];  c. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing;  d. Communicate incident response plan changes to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; and  e. Protect the incident response plan from unauthorized disclosure and modification. |  |  |
| IR-09  IR-09-01  IR-09-02  IR-09-03  IR-09-04 | IR-9 | INFORMATION SPILLAGE RESPONSE | Not Applicable for NIST Low-Impact Information Systems |  |  |
| IR-10 | IR-10 | INTEGRATED INFORMATION SECURITY ANALYSIS TEAM | [Withdrawn: Moved to IR-4(11).] |  |  |
| **Maintenance (MA)** | | | | | |
| MA-01 | MA-1 | POLICY AND PROCEDURES | a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:  1. [Selection (one or more): Organization-level; Mission/business process-level; System level] maintenance policy that:  (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and  (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and  2. Procedures to facilitate the implementation of the maintenance policy and the associated maintenance controls;  b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the maintenance policy and procedures; and  c. Review and update the current maintenance:  1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and  2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]. |  |  |
| MA-02  MA-02-02 | MA-2 | CONTROLLED MAINTENANCE | a. Schedule, document, and review records of maintenance, repair, and replacement on  system components in accordance with manufacturer or vendor specifications and/or organizational requirements;  b. Approve and monitor all maintenance activities, whether performed on site or remotely and whether the system or system components are serviced on site or removed to another location;  c. Require that [Assignment: organization-defined personnel or roles] explicitly approve the removal of the system or system components from organizational facilities for off-site maintenance, repair, or replacement;  d. Sanitize equipment to remove the following information from associated media prior to  removal from organizational facilities for off-site maintenance, repair, or replacement: [Assignment: organization-defined information];  e. Check all potentially impacted controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions; and  f. Include the following information in organizational maintenance records: [Assignment: organization-defined information]. |  |  |
| MA-03  MA-03-01  MA-03-02  MA-03-03 | MA-3 | MAINTENANCE TOOLS | Not Applicable for NIST Low-Impact Information Systems | Optional: (May be applicable for NIST Moderate or High Impact) |  |
| MA-04  MA-04-01  MA-04-02  MA-04-03  MA-04-06  MA-04-07 | MA-4 | NONLOCAL MAINTENANCE | a. Approve and monitor nonlocal maintenance and diagnostic activities;  b. Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system;  c. Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions;  d. Maintain records for nonlocal maintenance and diagnostic activities; and  e. Terminate session and network connections when nonlocal maintenance is completed. |  |  |
| MA-05  MA-05-01 | MA-5 | MAINTENANCE PERSONNEL | a. Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel;  b. Verify that non-escorted personnel performing maintenance on the system possess the required access authorizations; and  c. Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations. |  |  |
| MA-06 | MA-6 | TIMELY MAINTENANCE | Not Applicable | Optional: (May be applicable for NIST Moderate or High Impact) |  |
| **Media Protection (MP)** | | | | | |
| MP-01 | MP-1 | MEDIA PROTECTION POLICY AND PROCEDURES | a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:  1. [Selection (one or more): Organization-level; Mission/business process-level; System level] media protection policy that:  (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and  (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and  2. Procedures to facilitate the implementation of the media protection policy and the associated media protection controls;  b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the media protection policy and procedures; and  c. Review and update the current media protection:  1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and  2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]. |  |  |
| MP-02 | MP-2 | MEDIA ACCESS | Restrict access to [Assignment: organization-defined types of digital and/or non-digital media] to [Assignment: organization-defined personnel or roles]. |  |  |
| MP-03 | MP-3 | MEDIA MARKING | Not Applicable for NIST Low-Impact Information Systems | Optional: (May be applicable for NIST Moderate or High Impact) |  |
| MP-04 | MP-4 | MEDIA STORAGE | Not Applicable for NIST Low-Impact Information Systems | Optional: (May be applicable for NIST Moderate or High Impact) |  |
| MP-05  MP-05-04 | MP-5 | MEDIA TRANSPORT | Not Applicable for NIST Low-Impact Information Systems | Optional: (May be applicable for NIST Moderate or High Impact) |  |
| MP-06  MP-06-01  MP-06-02  MP-06-03 | MP-6 | MEDIA SANITIZATION | a. Sanitize [Assignment: organization-defined system media] prior to disposal, release out of organizational control, or release for reuse using [Assignment: organization-defined sanitization techniques and procedures]; and  b. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information. |  |  |
| MP-07  MP-07-01 | MP-7 | MEDIA USE | a. [Selection: Restrict; Prohibit] the use of [Assignment: organization-defined types of system media] on [Assignment: organization-defined systems or system components] using [Assignment: organization-defined controls]; and  b. Prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner. |  |  |
| **Physical and Environmental Protection (PE)** | | | | | |
| PE-01 | PE-1 | POLICY AND PROCEDURES | a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:  1. [Selection (one or more): Organization-level; Mission/business process-level; System level] physical and environmental protection policy that:  (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and  (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and  2. Procedures to facilitate the implementation of the physical and environmental protection policy and the associated physical and environmental protection controls;  b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures; and  c. Review and update the current physical and environmental protection:  1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and  2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]. |  |  |
| PE-02 | PE-2 | PHYSICAL ACCESS AUTHORIZATIONS | a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides;  b. Issue authorization credentials for facility access;  c. Review the access list detailing authorized facility access by individuals [Assignment: organization-defined frequency]; and  d. Remove individuals from the facility access list when access is no longer required. |  |  |
| PE-03  PE-03-01 | PE-3 | PHYSICAL ACCESS CONTROL | a. Enforce physical access authorizations at [Assignment: organization-defined entry and exit  points to the facility where the system resides] by:  1. Verifying individual access authorizations before granting access to the facility; and  2. Controlling ingress and egress to the facility using [Selection (one or more): [Assignment: organization-defined physical access control systems or devices]; guards];  b. Maintain physical access audit logs for [Assignment: organization-defined entry or exit points];  c. Control access to areas within the facility designated as publicly accessible by implementing the following controls: [Assignment: organization-defined physical access controls];  d. Escort visitors and control visitor activity [Assignment: organization-defined circumstances requiring visitor escorts and control of visitor activity];  e. Secure keys, combinations, and other physical access devices;  f. Inventory [Assignment: organization-defined physical access devices] every [Assignment:  organization-defined frequency]; and  g. Change combinations and keys [Assignment: organization-defined frequency] and/or when keys are lost, combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated. |  |  |
| PE-04 | PE-4 | ACCESS CONTROL FOR TRANSMISSION | Not Applicable for NIST Low-Impact Information Systems | Optional: (May be applicable for NIST Moderate or High Impact) |  |
| PE-05 | PE-5 | ACCESS CONTROL FOR OUTPUT DEVICES | Not Applicable for NIST Low-Impact Information Systems | Optional: (May be applicable for NIST Moderate or High Impact) |  |
| PE-06  PE-06-01  PE-06-04 | PE-6 | MONITORING PHYSICAL ACCESS | a. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents;  b. Review physical access logs [Assignment: organization-defined frequency] and upon occurrence of [Assignment: organization-defined events or potential indications of events]; and  c. Coordinate results of reviews and investigations with the organizational incident response capability |  |  |
| PE-08  PE-08-01 | PE-8 | VISITOR ACCESS RECORDS | a. Maintain visitor access records to the facility where the system resides for [Assignment: organization-defined time period];  b. Review visitor access records [Assignment: organization-defined frequency]; and  c. Report anomalies in visitor access records to [Assignment: organization-defined personnel]. |  |  |
| PE-09 | PE-9 | POWER EQUIPMENT AND POWER CABLING | Not Applicable for NIST Low-Impact Information Systems | Optional: (May be applicable for NIST Moderate or High Impact) |  |
| PE-10 | PE-10 | EMERGENCY SHUTOFF | Not Applicable for NIST Low-Impact Information Systems | Optional: (May be applicable for NIST Moderate or High Impact) |  |
| PE-11  PE-11-01 | PE-11 | EMERGENCY POWER | Not Applicable for NIST Low-Impact Information Systems | Optional: (May be applicable for NIST Moderate or High Impact) |  |
| PE-12 | PE-12 | EMERGENCY LIGHTING | Employ and maintain automatic emergency lighting for the system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility |  |  |
| PE-13  PE-13-01  PE-13-02  PE-13-03  PE-13-04 | PE-13 | FIRE PROTECTION | Employ and maintain fire detection and suppression systems that are supported by an independent energy source. |  |  |
| PE-14 | PE-14 | ENVIRONMENTAL CONTROLS | a. Maintain [Selection (one or more): temperature; humidity; pressure; radiation; [Assignment: organization-defined environmental control]] levels within the facility where the system resides at [Assignment: organization-defined acceptable levels]; and  b. Monitor environmental control levels [Assignment: organization-defined frequency]. |  |  |
| PE-15  PE-15-01 | PE-15 | WATER DAMAGE PROTECTION | Protect the system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel. |  |  |
| PE-16 | PE-16 | DELIVERY AND REMOVAL | a. Authorize and control [Assignment: organization-defined types of system components] entering and exiting the facility; and  b. Maintain records of the system components. |  |  |
| PE-17 | PE-17 | ALTERNATE WORK SITE | Not Applicable for NIST Low-Impact Information Systems | Optional: (May be applicable for NIST Moderate or High Impact) |  |
| PE-18 | PE-18 | LOCATION OF INFORMATION SYSTEM COMPONENTS | Not Applicable for NIST Low-Impact Information Systems | Optional: (May be applicable for NIST High Impact) |  |
| **Planning (PL)** | | | | | |
| PL-01 | PL-1 | POLICY AND PROCEDURES | a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:  1. [Selection (one or more): Organization-level; Mission/business process-level; System level] planning policy that:  (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and  (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and  2. Procedures to facilitate the implementation of the planning policy and the associated planning controls;  b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the planning policy and procedures; and  c. Review and update the current planning:  1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and  2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]. |  |  |
| PL-02  PL-02-03 | PL-2 | SYSTEM SECURITY AND PRIVACY PLANS | a. Develop security and privacy plans for the system that:  1. Are consistent with the organization’s enterprise architecture;  2. Explicitly define the constituent system components;  3. Describe the operational context of the system in terms of mission and business processes;  4. Identify the individuals that fulfill system roles and responsibilities;  5. Identify the information types processed, stored, and transmitted by the system;  6. Provide the security categorization of the system, including supporting rationale;  7. Describe any specific threats to the system that are of concern to the organization;  8. Provide the results of a privacy risk assessment for systems processing personally identifiable information;  9. Describe the operational environment for the system and any dependencies on or connections to other systems or system components;  10. Provide an overview of the security and privacy requirements for the system;  11. Identify any relevant control baselines or overlays, if applicable;  12. Describe the controls in place or planned for meeting the security and privacy  requirements, including a rationale for any tailoring decisions;  13. Include risk determinations for security and privacy architecture and design decisions;  14. Include security- and privacy-related activities affecting the system that require planning  and coordination with [Assignment: organization-defined individuals or groups]; and  15. Are reviewed and approved by the authorizing official or designated representative prior to plan implementation.  b. Distribute copies of the plans and communicate subsequent changes to the plans to [Assignment: organization-defined personnel or roles];  c. Review the plans [Assignment: organization-defined frequency];  d. Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments; and  e. Protect the plans from unauthorized disclosure and modification. |  |  |
| PL-04 | PL-4 | RULES OF BEHAVIOR | a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy;  b. Receive a documented acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system;  c. Review and update the rules of behavior [Assignment: organization-defined frequency]; and  d. Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge [Selection (one or more): [Assignment: organization-defined frequency]; when the rules are revised or updated]. |  |  |
| PL-04-01 | PL-4(1) | RULES OF BEHAVIOR | SOCIAL MEDIA AND EXTERNAL SITE/APPLICATION USAGE RESTRICTIONS | Include in the rules of behavior, restrictions on:  (a) Use of social media, social networking sites, and external sites/applications;  (b) Posting organizational information on public websites; and  (c) Use of organization-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications. |  |  |
| PL-08  PL-08-01  PL-08-02 | PL-8 | SECURITY AND PRIVACY ARCHITECTURES | Not Applicable for NIST Low-Impact Information Systems | Optional: (May be applicable for NIST Moderate or High Impact) |  |
| NA | PL-10 | BASELINE SELECTION | Select a control baseline for the system. |  |  |
| NA | PL-11 | BASELINE TAILORING | Tailor the selected control baseline by applying specified tailoring actions. |  |  |
| **Program Management (PM)** | | | | | |
| PM-01 | PM-1 | INFORMATION SECURITY PROGRAM PLAN | a. Develop and disseminate an organization-wide information security program plan that:  1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;  2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance;  3. Reflects the coordination among organizational entities responsible for information security; and  4. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation;  b. Review and update the organization-wide information security program plan [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and  c. Protect the information security program plan from unauthorized disclosure and modification. |  |  |
| PM-02 | PM-2 | INFORMATION SECURITY PROGRAM LEADERSHIP ROLE | Appoint a senior agency information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program. |  |  |
| PM-03 | PM-3 | INFORMATION SECURITY AND PRIVACY RESOURCES | a. Include the resources needed to implement the information security and privacy programs in capital planning and investment requests and document all exceptions to this requirement;  b. Prepare documentation required for addressing information security and privacy programs in capital planning and investment requests in accordance with applicable laws, executive orders, directives, policies, regulations, standards; and  c. Make available for expenditure, the planned information security and privacy resources. |  |  |
| PM-04 | PM-4 | PLAN OF ACTION AND MILESTONES PROCESS | a. Implement a process to ensure that plans of action and milestones for the information security, privacy, and supply chain risk management programs and associated organizational systems:  1. Are developed and maintained;  2. Document the remedial information security, privacy, and supply chain risk management actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and  3. Are reported in accordance with established reporting requirements.  b. Review plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions. |  |  |
| PM-05 | PM-5 | SYSTEM INVENTORY | Develop and update [Assignment: organization-defined frequency] an inventory of organizational systems. |  |  |
| PM-06 | PM-6 | MEASURES OF PERFORMANCE | Develop, monitor, and report on the results of information security and privacy measures of performance. |  |  |
| PM-07 | PM-7 | ENTERPRISE ARCHITECTURE | Develop and maintain an enterprise architecture with consideration for information security, privacy, and the resulting risk to organizational operations and assets, individuals, other organizations, and the Nation. |  |  |
| PM-08 | PM-8 | CRITICAL INFRASTRUCTURE PLAN | Address information security and privacy issues in the development, documentation,  and updating of a critical infrastructure and key resources protection plan. |  |  |
| PM-09 | PM-9 | RISK MANAGEMENT STRATEGY | a. Develops a comprehensive strategy to manage:  1. Security risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of organizational systems; and  2. Privacy risk to individuals resulting from the authorized processing of personally identifiable information;  b. Implement the risk management strategy consistently across the organization; and  c. Review and update the risk management strategy [Assignment: organization-defined frequency] or as required, to address organizational changes. |  |  |
| PM-10 | PM-10 | AUTHORIZATION PROCESS | a. Manage the security and privacy state of organizational systems and the environments in  which those systems operate through authorization processes;  b. Designate individuals to fulfill specific roles and responsibilities within the organizational risk  management process; and  c. Integrate the authorization processes into an organization-wide risk management program. |  |  |
| PM-11 | PM-11 | MISSION/ BUSINESS PROCESS DEFINITION | a. Define organizational mission and business processes with consideration for information  security and privacy and the resulting risk to organizational operations, organizational assets,  individuals, other organizations, and the Nation; and  b. Determine information protection and personally identifiable information processing needs  arising from the defined mission and business processes; and  c. Review and revise the mission and business processes [Assignment: organization-defined frequency]. |  |  |
| PM-12 | PM-12 | Insider Threat Program | Not Applicable for NIST Low-Impact Information Systems |  |  |
| PM-13 | PM-13 | Security and Privacy Workforce | Not Applicable for NIST Low-Impact Information Systems |  |  |
| PM-14 | PM-14 | Testing, Training, and Monitoring | Not Applicable for NIST Low-Impact Information Systems |  |  |
| PM-15 | PM-15 | Security and Privacy Groups and Associations | Not Applicable for NIST Low-Impact Information Systems |  |  |
| PM-16 | PM-16 | Threat Awareness Program | Not Applicable for NIST Low-Impact Information Systems |  |  |
| **Personnel Security (PS)** | | | | | |
| PS-01 | PS-1 | POLICY AND PROCEDURES | a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:  1. [Selection (one or more): Organization-level; Mission/business process-level; System level] personnel security policy that:  (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and  (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and  2. Procedures to facilitate the implementation of the personnel security policy and the associated personnel security controls;  b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the personnel security policy and procedures; and  c. Review and update the current personnel security:  1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and  2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]. |  |  |
| PS-02 | PS-2 | POSITION RISK DESIGNATION | a. Assign a risk designation to all organizational positions;  b. Establish screening criteria for individuals filling those positions; and  c. Review and update position risk designations [Assignment: organization-defined frequency]. |  |  |
| PS-03 | PS-3 | PERSONNEL SCREENING | a. Screen individuals prior to authorizing access to the system; and  b. Rescreen individuals in accordance with [Assignment: organization-defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of rescreening]. |  |  |
| PS-04  PS-04-01  PS-04-02 | PS-4 | PERSONNEL TERMINATION | a. Disable system access within [Assignment: organization-defined time period];  b. Terminate or revoke any authenticators and credentials associated with the individual;  c. Conduct exit interviews that include a discussion of [Assignment: organization-defined information security topics];  d. Retrieve all security-related organizational system-related property; and  e. Retain access to organizational information and systems formerly controlled by terminated individual. |  |  |
| PS-05 | PS-5 | PERSONNEL TRANSFER | a. Review and confirm ongoing operational need for current logical and physical access authorizations to systems and facilities when individuals are reassigned or transferred to other positions within the organization;  b. Initiate [Assignment: organization-defined transfer or reassignment actions] within [Assignment: organization-defined time period following the formal transfer action];  c. Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and  d. Notify [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period]. |  |  |
| PS-06  PS-06-03 | PS-6 | ACCESS AGREEMENTS | a. Develop and document access agreements for organizational systems;  b. Review and update the access agreements [Assignment: organization-defined frequency]; and  c. Verify that individuals requiring access to organizational information and systems:  1. Sign appropriate access agreements prior to being granted access; and  2. Re-sign access agreements to maintain access to organizational systems when access agreements have been updated or [Assignment: organization-defined frequency]. |  |  |
| PS-07 | PS-7 | EXTERNAL PERSONNEL SECURITY | a. Establish personnel security requirements, including security roles and responsibilities for external providers;  b. Require external providers to comply with personnel security policies and procedures established by the organization;  c. Document personnel security requirements;  d. Require external providers to notify [Assignment: organization-defined personnel or roles] of any personnel transfers or terminations of external personnel who possess organizational credentials and/or badges, or who have system privileges within [Assignment: organization defined time period]; and  e. Monitor provider compliance with personnel security requirements. |  |  |
| PS-08 | PS-8 | PERSONNEL SANCTIONS | a. Employ a formal sanctions process for individuals failing to comply with established  information security and privacy policies and procedures; and  b. Notify [Assignment: organization-defined personnel or roles] within [Assignment:  organization-defined time period] when a formal employee sanctions process is initiated,  identifying the individual sanctioned and the reason for the sanction. |  |  |
| NA | PS-9 | POSITION DESCRIPTIONS | Incorporate security and privacy roles and responsibilities into organizational position  descriptions. |  |  |
| **Risk Assessment (RA)** | | | | | |
| RA-01 | RA-1 | POLICY AND PROCEDURES | a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:  1. [Selection (one or more): Organization-level; Mission/business process-level; System level] risk assessment policy that:  (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and  (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and  2. Procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls;  b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the risk assessment policy and procedures; and  c. Review and update the current risk assessment:  1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and  2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]. |  |  |
| RA-02 | RA-2 | SECURITY CATEGORIZATION | a. Categorize the system and information it processes, stores, and transmits;  b. Document the security categorization results, including supporting rationale, in the security plan for the system; and  c. Verify that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision. |  |  |
| RA-03 | RA-3 | RISK ASSESSMENT | a. Conduct a risk assessment, including:  1. Identifying threats to and vulnerabilities in the system;  2. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and  3. Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information;  b. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments;  c. Document risk assessment results in [Selection: security and privacy plans; risk assessment report; [Assignment: organization-defined document]];  d. Review risk assessment results [Assignment: organization-defined frequency];  e. Disseminate risk assessment results to [Assignment: organization-defined personnel or roles]; and  f. Update the risk assessment [Assignment: organization-defined frequency] or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system. |  |  |
| NA | RA-3(1) | RISK ASSESSMENT | SUPPLY CHAIN RISK ASSESSMENT | (a) Assess supply chain risks associated with [Assignment: organization-defined systems, system components, and system services]; and  (b) Update the supply chain risk assessment [Assignment: organization-defined frequency], when there are significant changes to the relevant supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in the supply chain. |  |  |
| RA-05  RA-05-01  RA-05-04  RA-05-05  RA-05-10 | RA-5 | VULNERABILITY SCANNING | a. Monitor and scan for vulnerabilities in the system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system are identified and reported;  b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:  1. Enumerating platforms, software flaws, and improper configurations;  2. Formatting checklists and test procedures; and  3. Measuring vulnerability impact;  c. Analyze vulnerability scan reports and results from vulnerability monitoring;  d. Remediate legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk;  e. Share information obtained from the vulnerability monitoring process and control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other systems; and  f. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned. |  |  |
| RA-05-02 | RA-5(2) | VULNERABILITY MONITORING AND SCANNING | UPDATE VULNERABILITIES TO BE SCANNED | Update the system vulnerabilities to be scanned [Selection (one or more): [Assignment: organization-defined frequency]; prior to a new scan; when new vulnerabilities are identified and reported]. |  |  |
| NA | RA-5(11) | VULNERABILITY MONITORING AND SCANNING | PUBLIC DISCLOSURE PROGRAM | Establish a public reporting channel for receiving reports of vulnerabilities in organizational systems and system components. |  |  |
| NA | RA-7 | RISK RESPONSE | Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance. |  |  |
| **System and Services Acquisition (SA)** | | | | | |
| SA-01 | SA-1 | POLICY AND PROCEDURES | a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:  1. [Selection (one or more): Organization-level; Mission/business process-level; System level] system and services acquisition policy that:  (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and  (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and  2. Procedures to facilitate the implementation of the system and services acquisition policy and the associated system and services acquisition controls;  b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and services acquisition policy and procedures; and  c. Review and update the current system and services acquisition:  1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and  2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]. |  |  |
| SA-02 | SA-2 | ALLOCATION OF RESOURCES | a. Determine the high-level information security and privacy requirements for the system or system service in mission and business process planning;  b. Determine, document, and allocate the resources required to protect the system or system service as part of the organizational capital planning and investment control process; and  c. Establish a discrete line item for information security and privacy in organizational programming and budgeting documentation. |  |  |
| SA-03 | SA-3 | SYSTEM DEVELOPMENT LIFE CYCLE | a. Acquire, develop, and manage the system using [Assignment: organization-defined system development life cycle] that incorporates information security and privacy considerations;  b. Define and document information security and privacy roles and responsibilities throughout the system development life cycle;  c. Identify individuals having information security and privacy roles and responsibilities; and  d. Integrate the organizational information security and privacy risk management process into system development life cycle activities. |  |  |
| SA-04  SA-04-01  SA-04-02  SA-04-03  SA-04-05  SA-04-07  SA-04-09 | SA-4 | ACQUISITION Process | Include the following requirements, descriptions, and criteria, explicitly or by reference,  using [Selection (one or more): standardized contract language; [Assignment: organization defined contract language]] in the acquisition contract for the system, system component, or  system service:  a. Security and privacy functional requirements;  b. Strength of mechanism requirements;  c. Security and privacy assurance requirements;  d. Controls needed to satisfy the security and privacy requirements.  e. Security and privacy documentation requirements;  f. Requirements for protecting security and privacy documentation;  g. Description of the system development environment and environment in which the system  is intended to operate;  h. Allocation of responsibility or identification of parties responsible for information security,  privacy, and supply chain risk management; and   1. Acceptance criteria. |  |  |
| NA | SA-4(10) | ACQUISITION PROCESS | USE OF APPROVED PIV PRODUCTS | Employ only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational systems. |  |  |
| SA-05 | SA-5 | SYSTEM DOCUMENTATION | a. Obtain or develop administrator documentation for the system, system component, or system service that describes:  1. Secure configuration, installation, and operation of the system, component, or service;  2. Effective use and maintenance of security and privacy functions and mechanisms; and  3. Known vulnerabilities regarding configuration and use of administrative or privileged functions;  b. Obtain or develop user documentation for the system, system component, or system service that describes:  1. User-accessible security and privacy functions and mechanisms and how to effectively use those functions and mechanisms;  2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner and protect individual privacy; and  3. User responsibilities in maintaining the security of the system, component, or service and privacy of individuals;  c. Document attempts to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent and take [Assignment: organization-defined actions] in response; and  d. Distribute documentation to [Assignment: organization-defined personnel or roles]. |  |  |
| SA-08 | SA-8 | SECURITY DESIGN PRINCIPLES | Apply the following systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components: [Assignment: organization-defined systems security and privacy engineering principles]. |  |  |
| SA-09  SA-09-01  SA-09-02 | SA-9 | EXTERNAL SYSTEM SERVICES | a. Require that providers of external system services comply with organizational security and privacy requirements and employ the following controls: [Assignment: organization-defined controls];  b. Define and document organizational oversight and user roles and responsibilities with regard to external system services; and  c. Employ the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis: [Assignment: organization-defined processes, methods, and techniques]. |  |  |
| SA-10  SA-10-01 | SA-10 | DEVELOPER CONFIGURATION MANAGEMENT | Not Applicable for NIST Low-Impact Information Systems | Optional: (May be applicable for NIST Moderate or High Impact) |  |
| SA-11 | SA-11 | DEVELOPER TESTING AND EVALUATION | Not Applicable for NIST Low-Impact Information Systems | Optional: (May be applicable for NIST Moderate or High Impact) |  |
| SA-12  SA-12-01  SA-12-05  SA-12-08  SA-12-09 | SA-12 | SUPPLY CHAIN PROTECTION | [Withdrawn: Incorporated into SR Family.] |  |  |
| SA-14 | SA-14 | CRITICAL INFORMATION SYSTEM COMPONENTS | [Withdrawn: Incorporated into RA-9.] |  |  |
| SA-15  SA-15-03  SA-15-04  SA-15-07  SA-15-09 | SA-15 | DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | Not Applicable for NIST Low-Impact Information Systems | Optional: (May be applicable for NIST Moderate or High Impact) |  |
| SA-16 | SA-16 | DEVELOPER-PROVIDED TRAINING | Not Applicable for NIST Low-Impact Information Systems | Optional: (May be applicable for NIST High Impact) |  |
| SA-17 | SA-17 | DEVELOPER SECURITY AND PRIVACY ARCHITECTURE AND DESIGN | Not Applicable for NIST Low-Impact Information Systems | Optional: (May be applicable for NIST High Impact) |  |
| SA-19 | SA-19 | COMPONENT AUTHENTICITY | [Withdrawn: Moved to SR-11.] |  |  |
| NA | SA-21 | DEVELOPER SCREENING | Not Applicable for NIST Low-Impact Information Systems | Optional: (May be applicable for NIST High Impact) |  |
| SA-22 | SA-22 | UNSUPPORTED SYSTEM COMPONENTS | a. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; or  b. Provide the following options for alternative sources for continued support for unsupported components [Selection (one or more): in-house support; [Assignment: organization-defined support from external providers]]. |  |  |
| SA-23 | SA-23 | SPECIALIZATION | Not Applicable for NIST Low-Impact Information Systems |  |  |
| **System and Communications Protection (SC)** | | | | |  |
| SC-01 | SC-1 | POLICY AND PROCEDURES | a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:  1. [Selection (one or more): Organization-level; Mission/business process-level; System level] system and communications protection policy that:  (a) Addresses purpose, scope, roles, responsibilities, management commitment,  coordination among organizational entities, and compliance; and  (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and  2. Procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection controls;  b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and communications protection policy and procedures; and  c. Review and update the current system and communications protection:  1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and  2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]. |  |  |
| SC-02 | SC-2 | SEPARATION OF SYSTEM AND USER FUNCTIONALITY | Not Applicable for NIST Low-Impact Information Systems | Optional: (May be applicable for NIST Moderate or High Impact) |  |
| SC-03 | SC-3 | SECURITY FUNCTION ISOLATION | Not Applicable for NIST Low-Impact Information Systems | Optional: (May be applicable for NIST High Impact) |  |
| SC-04 | SC-4 | INFORMATION IN SHARED SYSTEM RESOURCES | Not Applicable for NIST Low-Impact Information Systems | Optional: (May be applicable for NIST Moderate or High Impact) |  |
| SC-05  SC-05-01  SC-05-02  SC-05-03 | SC-5 | DENIAL OF SERVICE PROTECTION | a. [Selection: Protect against; Limit] the effects of the following types of denial-of-service events: [Assignment: organization-defined types of denial-of-service events]; and  b. Employ the following controls to achieve the denial-of-service objective: [Assignment: organization-defined controls by type of denial-of-service event]. |  |  |
| SC-07  SC-07-03  SC-07-04  SC-07-05  SC-07-07  SC-07-08  SC-07-09  SC-07-10  SC-07-11  SC-07-12  SC-07-13  SC-07-14  SC-07-18  SC-07-21 | SC-7 | BOUNDARY PROTECTION | a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system;  b. Implement subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and  c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture. |  |  |
| SC-08  SC-08-01  SC-08-02 | SC-8 | TRANSMISSION CONFIDENTIALITY AND INTEGRITY | Not Applicable for NIST Low-Impact Information Systems | Optional: (May be applicable for NIST Moderate or High Impact) |  |
| SC-10 | SC-10 | NETWORK DISCONNECT | Not Applicable for NIST Low-Impact Information Systems | Optional: (May be applicable for NIST Moderate or High Impact) |  |
| SC-12  SC-12-01 | SC-12 | CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction]. |  |  |
| SC-13 | SC-13 | CRYPTOGRAPHIC PROTECTION | a. Determine the [Assignment: organization-defined cryptographic uses]; and  b. Implement the following types of cryptography required for each specified cryptographic use: [Assignment: organization-defined types of cryptography for each specified cryptographic use]. |  |  |
| SC-15 | SC-15 | COLLABORATIVE COMPUTING DEVICES AND APPLICATIONS | a. Prohibit remote activation of collaborative computing devices and applications with the following exceptions: [Assignment: organization-defined exceptions where remote activation is to be allowed]; and  b. Provide an explicit indication of use to users physically present at the devices. |  |  |
| SC-17 | SC-17 | PUBLIC KEY INFRASTRUCTURE CERTIFICATES | Not Applicable for NIST Low-Impact Information Systems | Optional: (May be applicable for NIST Moderate or High Impact) |  |
| SC-18  SC-18-01  SC-18-02  SC-18-03  SC-18-04 | SC-18 | MOBILE CODE | Not Applicable for NIST Low-Impact Information Systems | Optional: (May be applicable for NIST Moderate or High Impact) |  |
| SC-19 | SC-19 | VOICE OVER INTERNET PROTOCOL | [Withdrawn: Technology-specific; addressed as any other technology or protocol.] |  |  |
| SC-20 | SC-20 | SECURE NAME / ADDRESS RESOLUTION SERVICE (Authoritative Source) | a. Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and  b. Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace. |  |  |
| SC-21 | SC-21 | SECURE NAME / ADDRESS RESOLUTION SERVICE (Recursive or Caching Resolver) | Request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources. |  |  |
| SC-22 | SC-22 | ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE | Ensure the systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal and external role separation. |  |  |
| SC-23  SC-23-01  SC-23-03  SC-23-05 | SC-23 | SESSION AUTHENTICITY | Not Applicable for NIST Low-Impact Information Systems | Optional: (May be applicable for NIST Moderate or High Impact) |  |
| SC-24 | SC-24 | FAIL IN KNOWN STATE | Not Applicable for NIST Low-Impact Information Systems | Optional: (May be applicable for NIST High Impact) |  |
| SC-28  SC-28-01 | SC-28 | PROTECTION OF INFORMATION AT REST | Not Applicable for NIST Low-Impact Information Systems | Optional: (May be applicable for NIST Moderate or High Impact) |  |
| NA | SC-32 | SYSTEM PARTITIONING | Not Applicable for NIST Low-Impact Information Systems | Optional: (May be applicable for NIST Moderate or High Impact) |  |
| SC-38 | SC-38 | OPERATIONS SECURITY | Not Applicable for NIST Low-Impact Information Systems |  |  |
| SC-39 | SC-39 | PROCESS ISOLATION | Maintain a separate execution domain for each executing system process. |  |  |
| **System and Information integrity (SI)** | | | | | |
| SI-01 | SI-1 | POLICY AND PROCEDURES | a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:  1. [Selection (one or more): Organization-level; Mission/business process-level; System level] system and information integrity policy that:  (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and  (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and  2. Procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls;  b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and information integrity policy and procedures; and  c. Review and update the current system and information integrity:  1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and  2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]. |  |  |
| SI-02  SI-02-01  SI-02-02  SI-02-03  SI-02-06 | SI-2 | FLAW REMEDIATION | a. Identify, report, and correct system flaws;  b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;  c. Install security-relevant software and firmware updates within [Assignment: organization defined time period] of the release of the updates; and  d. Incorporate flaw remediation into the organizational configuration management process. |  |  |
| SI-03  SI-03-01  SI-03-02  SI-03-10 |  | MALICIOUS CODE PROTECTION | a. Implement [Selection (one or more): signature based; non-signature based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;  b. Automatically update malicious code protection mechanisms as new releases are available in  accordance with organizational configuration management policy and procedures;  c. Configure malicious code protection mechanisms to:  1. Perform periodic scans of the system [Assignment: organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more): endpoint; network entry and exit points] as the files are downloaded, opened, or executed in accordance with organizational policy; and  2. [Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]; and send alert to [Assignment: organization defined personnel or roles] in response to malicious code detection; and  d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system. |  |  |
| SI-04  SI-04-01  SI-04-02  SI-04-04  SI-04-05  SI-04-10  SI-04-11  SI-04-12  SI-04-14  SI-04-15  SI-04-16  SI-04-19  SI-04-20  SI-04-22  SI-04-23 | SI-4 | SYSTEM MONITORING | a. Monitor the system to detect:  1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]; and  2. Unauthorized local, network, and remote connections;  b. Identify unauthorized use of the system through the following techniques and methods: [Assignment: organization-defined techniques and methods];  c. Invoke internal monitoring capabilities or deploy monitoring devices:  1. Strategically within the system to collect organization-determined essential information; and  2. At ad hoc locations within the system to track specific types of transactions of interest to the organization;  d. Analyze detected events and anomalies;  e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation;  f. Obtain legal opinion regarding system monitoring activities; and  g. Provide [Assignment: organization-defined system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]]. |  |  |
| SI-05  SI-05-01 | SI-5 | SECURITY ALERTS, ADVISORIES, AND DIRECTIVES | a. Receive system security alerts, advisories, and directives from [Assignment: organization defined external organizations] on an ongoing basis;  b. Generate internal security alerts, advisories, and directives as deemed necessary;  c. Disseminate security alerts, advisories, and directives to: [Selection (one or more):[Assignment: organization-defined personnel or roles]; [Assignment: organization-defined elements within the organization]; [Assignment: organization-defined external organizations]]; and  d. Implement security directives in accordance with established time frames, or notify the issuing organization of the degree of noncompliance. |  |  |
| SI-06  SI-06-03 | SI-6 | SECURITY AND PRIVACY FUNCTION VERIFICATION | Not Applicable for NIST Low-Impact Information Systems | Optional: (May be applicable for NIST High Impact) |  |
| SI-07  SI-07-01  SI-07-02  SI-07-05  SI-07-07  SI-07-08  SI-07-14 | SI-7 | SOFTWARE AND INFORMATION INTEGRITY | Not Applicable for NIST Low-Impact Information Systems | Optional: (May be applicable for NIST Moderate or High Impact) |  |
| SI-08  SI-08-01  SI-08-02 | SI-8 | SPAM PROTECTION | Not Applicable for NIST Low-Impact Information Systems | Optional: (May be applicable for NIST Moderate or High Impact) |  |
| SI-10  SI-10-3 | SI-10 | INFORMATION INPUT VALIDATION | Not Applicable for NIST Low-Impact Information Systems | Optional: (May be applicable for NIST Moderate or High Impact) |  |
| SI-11 | SI-11 | ERROR HANDLING | Not Applicable for NIST Low-Impact Information Systems | Optional: (May be applicable for NIST Moderate or High Impact) |  |
| SI-12 | SI-12 | INFORMATION MANAGEMENT AND RETENTION | Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines and operational requirements. |  |  |
| SI-16 | SI-16 | MEMORY PROTECTION | Not Applicable for NIST Low-Impact Information Systems | Optional: (May be applicable for NIST Moderate or High Impact) |  |
| **SUPPLY CHAIN RISK MANAGEMENT (SR)** | | | | | |
| NA | SR-1 | POLICY AND PROCEDURES | a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:  1. [Selection (one or more): Organization-level; Mission/business process-level; System level] supply chain risk management policy that:  (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and  (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and  2. Procedures to facilitate the implementation of the supply chain risk management policy and the associated supply chain risk management controls;  b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the supply chain risk management policy and procedures; and  c. Review and update the current supply chain risk management:  1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and  2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]. |  |  |
| NA | SR-2 | SUPPLY CHAIN RISK MANAGEMENT PLAN | a. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the following systems, system components or system services:[Assignment: organization-defined systems, system components, or system services];  b. Review and update the supply chain risk management plan [Assignment: organization defined frequency] or as required, to address threat, organizational or environmental changes; and  c. Protect the supply chain risk management plan from unauthorized disclosure and modification. |  |  |
| NA | SR-2-1 | SUPPLY CHAIN RISK MANAGEMENT PLAN | ESTABLISH SCRM TEAM | Establish a supply chain risk management team consisting of [Assignment: organization defined personnel, roles, and responsibilities] to lead and support the following SCRM activities: [Assignment: organization-defined supply chain risk management activities]. |  |  |
| NA | SR-3 | SUPPLY CHAIN CONTROLS AND PROCESSES | a. Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of [Assignment: organization-defined system or system component] in coordination with [Assignment: organization-defined supply chain personnel];  b. Employ the following controls to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain related events: [Assignment: organization-defined supply chain controls]; and  c. Document the selected and implemented supply chain processes and controls in [Selection: security and privacy plans; supply chain risk management plan; [Assignment: organization defined document]]. |  |  |
| NA | SR-5 | ACQUISITION STRATEGIES, TOOLS, AND METHODS | Employ the following acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks: [Assignment: organization-defined acquisition strategies, contract tools, and procurement methods]. |  |  |
| NA | SR-6 | SUPPLIER ASSESSMENTS AND REVIEWS | Not Applicable for NIST Low-Impact Information Systems | Optional: (May be applicable for NIST Moderate or High Impact) |  |
| NA | SR-8 | NOTIFICATION AGREEMENTS | Establish agreements and procedures with entities involved in the supply chain for the system, system component, or system service for the [Selection (one or more): notification of supply chain compromises; results of assessments or audits; [Assignment: organization-defined information]]. |  |  |
| NA | SR-9 | TAMPER RESISTANCE AND DETECTION | Not Applicable for NIST Low-Impact Information Systems | Optional: (May be applicable for NIST High Impact) |  |
| NA | SR-10 | INSPECTION OF SYSTEMS OR COMPONENTS | Inspect the following systems or system components [Selection (one or more): at random; at [Assignment: organization-defined frequency], upon [Assignment: organization defined indications of need for inspection]] to detect tampering: [Assignment: organization defined systems or system components]. |  |  |
| NA | SR-11 | COMPONENT AUTHENTICITY | a. Develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system; and  b. Report counterfeit system components to [Selection (one or more): source of counterfeit component; [Assignment: organization-defined external reporting organizations];[Assignment: organization-defined personnel or roles]]. |  |  |
| NA | SR-11(1) | COMPONENT AUTHENTICITY | ANTI-COUNTERFEIT TRAINING | Train [Assignment: organization-defined personnel or roles] to detect counterfeit system components (including hardware, software, and firmware). |  |  |
| NA | SR-11(2) | COMPONENT AUTHENTICITY | CONFIGURATION CONTROL FOR COMPONENT SERVICE AND REPAIR | Maintain configuration control over the following system components awaiting service or repair and serviced or repaired components awaiting return to service: [Assignment: organization-defined system components]. |  |  |
| NA | SR-12 | COMPONENT DISPOSAL | Dispose of [Assignment: organization-defined data, documentation, tools, or system components] using the following techniques and methods: [Assignment: organization-defined techniques and methods]. |  |  |