Control	Control Name	Control Requirements	Updated Question(s) / Questions to add
AC-01	(Access Control) Policy and Procedures	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].	1. Is this control applicable for the information system? 2. Has an information system access control policy and procedures, which cover all information systems within the security boundary, been developed and disseminated to all employees? 3. Is there a person designated to manage the development, documentation, and dissemination of the policy and procedures? 4. Do the policies and procedures address all of the following (purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance)? 5. Are the policies and procedures consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines? 6. What is the frequency that the policies and procedures are reviewed and updated, if needed, by management?

AC-02	Account Management	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.	1. Is this control applicable for the information system? 2. For each information system within the security boundary, have account management procedures been developed? 3. Do the procedures address all of the following? Specify: Authorized users of the system; Group and role membership; and Access authorizations (i.e., privileges) and [Assignment: organization-defined attributes (as required)] for each account; Require approvals by [Assignment: organization-defined personnel or roles] for requests to create accounts; Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, prerequisites, and criteria]; Monitor the use of accounts; Notify account managers and [Assignment: organization-defined personnel or roles] within: [Assignment: organization-defined time period] when accounts are no longer required; [Assignment: organization-defined time period] when users are terminated or transferred; and [Assignment: organization-defined time period] when system usage or need-to-know changes for an individual; Is system access authorized based on: A valid access authorization; Intended system usage; and [Assignment: organization-defined attributes (as required)]; Review accounts for compliance with account management requirements [Assignment: organization-defined frequency]; Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and Align account management processes with personnel termination and transfer processes.
AC-02(1)	Account Management | Automated System Account Management	Support the management of system accounts using [Assignment: organization-defined automated mechanisms].	1. Is this control applicable for the information system? 2. Are automated mechanisms in place to support the management of system accounts?

AC-02(13)	Account Management | Disable Accounts for High-Risk Individuals	Disable accounts of individuals within [Assignment: organization-defined time period] of discovery of [Assignment: organization-defined significant risks].	1. Is this control applicable for the information system? 2. Are accounts disabled within the organizational defined time of discovery after significant risks are identified?
AC-02(2)	Account Management | Automated Temporary and Emergency Account Management	Automatically [Selection: remove; disable] temporary and emergency accounts after [Assignment: organization-defined time period for each type of account].	1. Is this control applicable for the information system? 2. Are automated mechanisms in place to remove or disable temporary or emergency accounts?
AC-02(3)	Account Management | Disable Accounts	Disable accounts within [Assignment: organization-defined time period] when the accounts: (a) Have expired; (b) Are no longer associated with a user or individual; (c) Are in violation of organizational policy; or (d) Have been inactive for [Assignment: organization-defined time period].	1. Is this control applicable for the information system? 2. Are accounts disabled within the organization-defined period when: (a) Have expired; (b) Are no longer associated with a user or individual; (c) Are in violation of organizational policy; or (d) Have been inactive for [Assignment: organization-defined time period]
AC-02(4)	Account Management | Automated Audit Actions	Automatically audit account creation, modification, enabling, disabling, and removal actions.	1. Is this control applicable for the information system? 2. Are automated mechanisms in place to audit account creation, modification, enabling, disabling, and removal actions?
AC-02(5)	Account Management | Inactivity Logout	Require that users log out when [Assignment: organization-defined time period of expected inactivity or description of when to log out].	1. Is this control applicable for the information system? 2. Are users logged out after organizational- defined time period?

AC-03	Access Enforcement	Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	1. Is this control applicable for the information system? 2. Is access approved for authorizations for logical access to information and system resources in accordance with applicable access control policies?
AC-03(14)	Access Enforcement | Individual Access	Provide [Assignment: organization-defined mechanisms] to enable individuals to have access to the following elements of their personally identifiable information: [Assignment: organization-defined elements].	1. Is this control applicable for the information system? 2. Are mechanisms in place to enable individuals to have access to their personally identifiable information within the information system?
AC-04	Information Flow Enforcement	Enforce approved authorizations for controlling the flow of information within the system and between connected systems based on [Assignment: organization-defined information flow control policies].	1. Is this control applicable for the information system? 2. For each information system within the security boundary, are interconnections documented and the flow of information between information systems restricted?
AC-05	Separation of Duties	a. Identify and document [Assignment: organization-defined duties of individuals requiring separation]; and b. Define system access authorizations to support separation of duties.	1. Is this control applicable for the information system? 2. For each information system within the security boundary, are there defined and documented separation of duties? 3. Have the system access authorizations that support the separation of duties been documented?
AC-06	Least Privilege	Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.	1. Is this control applicable for the information system? 2. For individuals with elevated privileges (e.g., system administration), are they required to use separate accounts to access privileged and non-privileged functions?

AC-06(1)	Least Privilege | Authorize Access to Security Functions	Authorize access for [Assignment: organization-defined individuals or roles] to: (a) [Assignment: organization-defined security functions (deployed in hardware, software, and firmware)]; and (b) [Assignment: organization-defined security-relevant information].	1. Is this control applicable for the information system? 2. Are their system accounts for users with elevated privileges?
AC-06(10)	Least Privilege | Prohibit Non-Privileged Users From Executing Privileged Functions	Prevent non-privileged users from executing privileged functions.	1. Is this control applicable for the information system? 2. Are non-privileged accounts prevented from executing privileged functions?
AC-06(2)	Least Privilege | Non-Privileged Access for Non-Security Functions	Require that users of system accounts (or roles) with access to [Assignment: organization-defined security functions or security-relevant information] use non-privileged accounts or roles, when accessing nonsecurity functions.	1. Is this control applicable for the information system? 2. For individuals with elevated privileges, do they have a non-privileged accounts to perform non-security functions?
AC-06(5)	Least Privilege | Privileged Accounts	Restrict privileged accounts on the system to [Assignment: organization-defined personnel or roles].	1. Is this control applicable for the information system? 2. Are system accounts with elevated privileges restricted based on the users' role?
AC-06(7)	Least Privilege | Review of User Privileges	(a) Review [Assignment: organization-defined frequency] the privileges assigned to [Assignment: organization-defined roles or classes of users] to validate the need for such privileges; and (b) Reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs.	1. Is this control applicable for the information system? 2. Are accounts with elevated privileges periodically reviewed to validate access is still required? 3. Are the accounts with elevated privileges reassigned or removed based on the periodic review?
AC-06(9)	Least Privilege | Log Use of Privileged Functions	Log the execution of privileged functions.	1. Is this control applicable for the information system? 2. Are logs captured for accounts with elevated access?

AC-07	Unsuccessful Logon 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.	1. Is this control applicable for the information system? 2. For each information system within the security boundary, does the information system automatically lock an account after 3 consecutive invalid login attempts? 3. Are system administrators notified when the maximum number of unsuccessful attempts is exceeded on an account?
AC-08	System Use Notification	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.	1.Is this control applicable for the information system? 2. For each information system within the security boundary, does the system display a notification message, as indicated in the control information, prior to granting access? 3. Are there public facing information systems within the security boundary?

AC-11	Device Lock	a. Prevent further access to the system by [Selection (one or more): initiating a device lock after [Assignment: organization-defined time period] of inactivity; requiring the user to initiate a device lock before leaving the system unattended]; and b. Retain the device lock until the user reestablishes access using established identification and authentication procedures.	1. Is this control applicable for the information system? 2. For each information system within the security boundary, does the information system initiate a session lock after a period of inactivity?
AC-11(1)	Device Lock | Pattern-Hiding Displays	Conceal, via the device lock, information previously visible on the display with a publicly viewable image.	1. Is this control applicable for the information system? 2. For each information system within the security boundary, when the session is locked does it conceal the contents that were visible on the display?
AC-12	Session Termination	Automatically terminate a user session after [Assignment: organization-defined conditions or trigger events requiring session disconnect].	1. Is this control applicable for the information system? 2. Conditions or trigger events requiring automatic session termination can include, for example, organization-defined periods of user inactivity, targeted responses to certain types of incidents, or time-of-day restrictions on information system use. For each information system within the security boundary, does the information system automatically terminate user sessions after a defined conditions or trigger events? 3. Does the information system terminate the user session after?
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.	1. Is this control applicable for the information system? 2. For each information system within the security boundary, are users able to perform any actions or functions without logging on first? 3. Are the user actions not requiring an initial logon documented?

AC-17	Remote Access	a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and b. Authorize each type of remote access to the system prior to allowing such connections.	1. Is this control applicable for the information system? 2. For each information system within the security boundary, are users authorized remote access (i.e., through external networks such as the Internet, dial-up, etc.)?
AC-17(1)	Remote Access | Monitoring and Control	Employ automated mechanisms to monitor and control remote access methods.	1. Is this control applicable for the information system? 2. Are automated mechanisms in place to monitor and control users authorized remote access?
AC-17(2)	Remote Access | Protection of Confidentiality and Integrity Using Encryption	Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.	1. Is this control applicable for the information system? 2. Are FIPS 140-2 cryptographic mechanisms used for remote access? 3. Are the cryptographic mechanisms FIPS 140-2 compliant?
AC-17(3)	Remote Access | Managed Access Control Points	Route remote accesses through authorized and managed network access control points.	1. Is this control applicable for the information system? 2. Is remote access routed through authorized and managed network access control points?
AC-17(4)	Remote Access | Privileged Commands and Access	(a) Authorize the execution of privileged commands and access to security-relevant information via remote access only in a format that provides assessable evidence and for the following needs: [Assignment: organization-defined needs]; and (b) Document the rationale for remote access in the security plan for the system.	1. Is this control applicable for the information system? 2. Is the execution of privilege commands and access to security-relevant information via remote access restricted to authorized individuals and also documented?

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.	1. Is this control applicable for the information system? 2. Is wireless access to information systems explicitly approved by management? 3. Have usage restrictions, configuration/connection requirements (i.e., encryption enabled, access points in secured areas, personal firewalls, etc.) and implementation guidance been documented and approved by management? 4. Are users and / or devices required to authenticate prior to obtaining access?
AC-18(1)	Wireless Access | Authentication and Encryption	Protect wireless access to the system using authentication of [Selection (one or more): users; devices] and encryption.	1. Is this control applicable for the information system? 2. Have usage restrictions, configuration/connection requirements (i.e., encryption enabled, access points in secured areas, personal firewalls, etc.) and implementation guidance been documented and approved by management?
AC-18(3)	Wireless Access | Disable Wireless Networking	Disable, when not intended for use, wireless networking capabilities embedded within system components prior to issuance and deployment.	1. Is this control applicable for the information system? 2. Are wireless networking capabilities that are not intended for use disabled within system components prior to issuance and deployment?
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.	1. Is this control applicable for the information system? 2. Are mobile devices authorized to access the information systems within the security boundary? 3. Have usage restrictions, configuration/connection requirements and implementation guidance for mobile device access been documented and approved by management?
AC-19(5)	Access Control for Mobile Devices | Full Device or Container-Based Encryption	Employ [Selection: full-device encryption; container-based encryption] to protect the confidentiality and integrity of information on [Assignment: organization-defined mobile devices].	1. Is this control applicable for the information system? 2. Has one or more encryption type on mobile devices been employed?

AC-20	Use of External 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].	1. Is this control applicable for the information system? 2. For each information system within the security boundary, have external information systems been authorized by management to access, process, store and/or transmit organizational information?
AC-20(1)	Use of External Systems | Limits On Authorized Use	Permit authorized individuals to use an external system to access the system or to process, store, or transmit organization-controlled information only after: (a) Verification of the implementation of controls on the external system as specified in the organization's security and privacy policies and security and privacy plans; or (b) Retention of approved system connection or processing agreements with the organizational entity hosting the external system.	1. Is this control applicable for the information system? 2. Has management verified the implementation of security controls on external systems to be equivalent as required by the owning/hosting organization? And, are those agreements with external information systems retained by management?
AC-20(2)	Use of External Systems | Portable Storage Devices – Restricted Use	Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems using [Assignment: organization-defined restrictions].	1. Is this control applicable for the information system? 2. Are the use of organizational-controlled portable storage devices either?

AC-21	Information Sharing	a. Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions for [Assignment: organization-defined information sharing circumstances where user discretion is required]; and b. Employ [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing and collaboration decisions.	1. Is this control applicable for the information system? 2. Is information shared with partners or other organizations? 3. Have policies and procedures been enabled so authorized users can determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for approved information-sharing circumstances where user discretion is required? 4. Are automated systems used to assist users in making information sharing collaboration decisions?
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.	1. Is this control applicable for the information system? 2. For publicly accessible content, have designated individuals been authorized to post information onto a publicly accessible information system? 3. Are authorized individuals trained to ensure that publicly accessible information does not contain nonpublic information?

AT-01	(Awareness and Training) 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].	1. Is this control applicable for the information system? 2. Has an information system awareness and training policy and procedures, which cover all information systems within the security boundary, been developed and disseminated to all employees? 3. Is there a person designated to manage the development, documentation, and dissemination of the policy and procedures? 4. Do the policies and procedures address all of the following (purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance)? 5. Are the policies and procedures consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines? 6. What is the frequency that the policies and procedures are reviewed and updated, if needed, by management?

AT-02	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.	1. Is this control applicable for the information system? 2. Is security and privacy literacy training to information system users (including managers, senior executives, and contractors) provided? 3. Is security and privacy literacy training required as part of initial training from users? 4. Is security and privacy literacy training required annually thereafter? 5. Is security and privacy literacy training required by system change? 6.Is security and privacy literacy training content updated? 7. Are lessons learned conducted to incorporate training content for external or internal security incidents or breaches?
AT-02(2)	Literacy Training and Awareness | Insider Threat	Provide literacy training on recognizing and reporting potential indicators of insider threat.	1. Is this control applicable for the information system? 2. Is security awareness training on recognizing and reporting potential indicators of insider threat included in the organization`s basic security awareness training?
AT-02(3)	Literacy Training and Awareness | Social Engineering and Mining	Provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining.	1. Is this control applicable for the information system? 2. Is literacy training provided to recognize and report potential and actual instances of social engineering and social mining?

AT-03	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.	1. Is this control applicable for the information system? 2. Is role-based security and privacy training provided to personnel with assigned security roles and responsibilities? 3. Is role-based security and privacy training required for designated personnel before authorizing access to the information system or performing assigned duties? 5. Is role-based security and privacy training required for designated personnel on an annual basis? 6. Are lessons learned conducted to incorporate training content for external or internal security incidents or breaches?
AT-03(5)	Role-Based Training | Processing Personally Identfiable Information	Provide [Assignment: organization-defined personnel or roles] with initial and [Assignment: organization-defined frequency] training in the employment and operation of personally identifiable information processing and transparency controls.	1. Is this control applicable for the information system? 2. Is role-based training provided in the use and operation of personally identifiable information processing and transparency?
AT-04	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].	1. Is this control applicable for the information system? 2. Are individual information system security and privacy training activities documented and retained for one (1) year?

AU-01	(Audit and Accountability) 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].	1. Is this control applicable for the information system? 2. Is there an audit and accountability policy? 3. Does the audit policy address all of the following? (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 4. Are there procedures for audit and accountability? 5. Are the procedures for audit and accountability updated annually?

AU-02	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].	1. Is this control applicable for the information system? 2. Has the information system identified the types of events the system is capable of logging in support of the audit function? 3. Have the event types for logging within the system along with the frequency been identified and documented? 4. Have the event types been reviewed and updated?
AU-03	Content of Audit Records	Control: 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.	1. Is this control applicable for the information system? 2. Does the information system audit all of the following event types? 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-03(1)	Content of Audit Records | Additional Audit Information	Generate audit records containing the following additional information: [Assignment: organization-defined additional information].	1. Is this control applicable for the information system? 2. Do audit records contain the following information: Type of event? When the event occurred? Where the event occurred? The source of the event? Event outcome/end state? Individual or agent associated with the event?
AU-03(3)	Content of Audit Records | Limit Personally Identifiable Information Elements	Limit personally identifiable information contained in audit records to the following elements identified in the privacy risk assessment: [Assignment: organization-defined elements].	1. Is this control applicable for the information system? 2. Is PII included in audit records?
AU-04	Audit Log Storage Capacity	Allocate audit log storage capacity to accommodate [Assignment: organization-defined audit log retention requirements].	1. Is this control applicable for the information system? 2. Does the information system allocate sufficient storage for two years of audit logs?
AU-05	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].	1. Is this control applicable for the information system? 2.Does the information system provide notifications in the event of audit processing failure? 3. Are the network manager and CIO notified of audit processing failure?
AU-06	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.	1. Is this control applicable for the information system? 2. The organization reviews the audit records for indications of inappropriate or unusual activity weekly? 3. If yes, are their management level reviews the audit records for indications of inappropriate or unusual activity quarterly?

AU-06(1)	Audit Record Review, Analysis, and Reporting | Automated Process Integration	Integrate audit record review, analysis, and reporting processes using [Assignment: organization-defined automated mechanisms].	1. Is this control applicable for the information system? 2. Are automated mechanisms used to support all audit activities below: review? analysis? reporting? 3. Are findings reported to the Security Manager and CIO?
AU-06(3)	Audit Record Review, Analysis, and Reporting | Correlate Audit Record Repositories	Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.	1. Is this control applicable for the information system? 2. Are audit records analyzed and correlated across different repositories to gain situational awareness?
AU-07	Audit Record Reduction and Report Generation	Provide and implement an audit record reduction and report generation capability that: a. Supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of incidents; and b. Does not alter the original content or time ordering of audit records.	1. Is this control applicable for the information system? 2. Does the information system have an audit reduction and report creation capacity?
AU-07(1)	Audit Record Reduction and Report Generation | Automatic Processing	Provide and implement the capability to process, sort, and search audit records for events of interest based on the following content: [Assignment: organization-defined fields within audit records].	1. Is this control applicable for the information system? 2. Does that audit report tool support on-demand: audit review? analysis? reporting requirements? 3. Can the information system filter audit records for events of interest, based on any or all of the audit fields? 4. Does the audit report tool prevent: alteration of original contents or alteration of time lines of records?

AU-08	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.	1. Is this control applicable for the information system? 2. Does the information system apply time stamps to audit records? 3. Are time stamps determined by: Using internal clocks Mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT)? 4. Does the information system perform all of the below activities: Compare the internal clocks every 64 seconds with the time.nest.gov time? Synchronize the internal system clocks with the authoritative time source when the time difference exceeds one second?
AU-09	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.	1. Is this control applicable for the information system? 2. Does the information system protect the following from unauthorized access, modification, and deletion: audit information? audit tools? 3. Do IT staff member receive alerts upon detection of unauthorized access, modification, or deletion of audit information?
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.	1. Is this control applicable for the information system? 2. Does the organization retain audit records for two years?
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.	1. Is this control applicable for the information system? 2. Does the information system provide audit records for the list of auditable events in AU-2 for: all systems which handle confidential information? accept network connections? provide access control? 3. Does the information system allow authorized personnel to select which auditable events are to be captured by specific components? 4. Does the information system generate audit records for all the audit events listed previously?

AU-9(4)	Protection of Audit Information | Access By Subset of Privileged Users	Authorize access to management of audit logging functionality to only [Assignment: organization-defined subset of privileged users or roles].	1. Is this control applicable for the information system? 2. Does the organization limit access to audit management to only the Network manager, CIO, and other IT staff?
CA-01	(Assessment, Authorization, and Monitoring) 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].	1. Is this control applicable for the information system? 2. Has an information system assessment, authorization, and monitoring policy and procedures, been developed and disseminated to all employees? 3. Is there a person designated to manage the development, documentation, and dissemination of the policy and procedures? 4. Do the policies and procedures address all of the following (purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance)? 5. Are the policies and procedures consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines? 6. What is the frequency that the policies and procedures are reviewed and updated, if needed, by management? 7. What events require an updates to the policy and procedures?

CA-02	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].	1. Is this control applicable for the information system? 2. Have the appropriate assessor or assessment team for the type of assessment to be conducted been selected? 3. Is there a security assessment plan? Does the security assessment plan describe the scope of the assessment including all of the following? a. Controls and control enhancements under assessment; b. Assessment procedures to be used to determine control effectiveness; and c. Assessment environment, assessment team, and assessment roles and responsibilities; d. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment; e. 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; f. Produce a control assessment report that document the results of the assessment; and g. Provide the results of the control assessment to [Assignment: organization-defined individuals or roles].
CA-02(1)	Control Assessments | Independent Assessors	Employ independent assessors or assessment teams to conduct control assessments.	1. Is this control applicable for the information system? 2. Do independent assessors or assessment teams conduct control assessments?

CA-03	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].	1. Is this control applicable for the information system? 2. Are connections from the information system to other information systems authorized through the use of Interconnection Security Agreements (ISA)? 3. Do Interconnection Security Agreements (ISA) include the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated? 4. Are Interconnection Security Agreements (ISA) reviewed and updated?
CA-05	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.	1. Is this control applicable for the information system? 2. Is there a plan of action and milestones (POA&M) for the information system to document the organization`s planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security control and to reduce or eliminate known vulnerabilities in the system?
CA-06	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].	1. Is this control applicable for the information system? 2. Is a senior-level executive or manager assigned as the authorizing official for the for common controls available for inheritance by organizational systems? 3. Is a senior-level executive or manager assigned as the authorizing official for the information system? 4. Does the authorizing officer authorize the information system for processing before commencing operations? 5. Is the security authorization updated every 3 years or whenever a major change occurs?

CA-07	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].	1. Is this control applicable for the information system? 2. Is there a continuous monitoring strategy in place? 3. Is there a continuous monitoring program? 4. Does the continuous monitoring program include all of the following requirements? 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] 5. Are independent assessors or assessment teams employed to monitor the security controls in the information system on an ongoing basis?
CA-07(1)	Continuous Monitoring | Independent Assessment	Employ independent assessors or assessment teams to monitor the controls in the system on an ongoing basis.	1. Is this control applicable for the information system? 2. Do independent assessors or assessment teams monitor the controls in the system on an ongoing basis?

CA-07(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.	1. Is this control applicable for the information system? 2. Is risk monitored as an integral part of the continuous monitoring strategy that includes the following: (a) Effectiveness monitoring; (b) Compliance monitoring; and (c) Change monitoring.
CA-09	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.	1. Is this control applicable for the information system? 2. Are internal connections agreements authorized to the information system? Example - Non-FSA systems that interconnect with your FSA specific systems within the organization. Are those connections authorized? 3. For each internal connection, have the interface characteristics, security and privacy requirements, and the nature of the information communicated been documented? 4. When are internal system connections terminated? 5. Are internal connections periodically reviewed to ensure they are still needed?

CM-01	(Configuration Management) 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].	1. Is this control applicable for the information system? 2. Is there a configuration management policy? 3. Does the configuration management policy address all requirements below? (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; 4. Is the configuration management policy updated annually? 5. Is there a designated personnel to manage the development, documentation, and dissemination of the configuration management policy and procedures? 6. Is there a configuration management procedure?
CM-02	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.	1. Is this control applicable for the information system? 2. Is there a current baseline configuration for the system? 3. Is the baseline configuration documented and maintained in a repository? 4. Is the configuration baseline reviewed and/or updated at the following frequencies: Annually When required due to network/infrastructure upgrades or changes? 5. Are individuals travelling to locations of significant risk issued information system components with special configurations?

CM-02(2)	Baseline Configuration | Automation Support for Accuracy and Currency	Maintain the currency, completeness, accuracy, and availability of the baseline configuration of the system using [Assignment: organization-defined automated mechanisms].	1. Is this control applicable for the information system? 2. Are automated mechanisms in place to maintain the currency, completeness, accuracy, and availability of the baseline configuration of the system?
CM-02(3)	Baseline Configuration | Retention of Previous Configurations	Retain [Assignment: organization-defined number] of previous versions of baseline configurations of the system to support rollback.	1. Is this control applicable for the information system? 2. Are previous versions of the baseline retained for roll-back, including diagrams and organization-defined configurations?
CM-02(7)	Baseline Configuration | Configure Systems and Components for High-Risk Areas	(a) Issue [Assignment: organization-defined systems or system components] with [Assignment: organization-defined configurations] to individuals traveling to locations that the organization deems to be of significant risk; and (b) Apply the following controls to the systems or components when the individuals return from travel: [Assignment: organization-defined controls].	1. Is this control applicable for the information system? 2. Are systems and/or components configured to organizational standards when individuals are traveling to high risk areas? 3. What controls are applied to systems and/or components when individuals return from high risk travel areas?

CM-03	Configuration Change Control	a. Determine and document the types of changes to the system that are configuration-controlled; b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses; c. Document configuration change decisions associated with the system; d. Implement approved configuration-controlled changes to the system; e. Retain records of configuration-controlled changes to the system for [Assignment: organization-defined time period]; f. Monitor and review activities associated with configuration-controlled changes to the system; and g. Coordinate and provide oversight for configuration change control activities through [Assignment: organization-defined configuration change control element] that convenes [Selection (one or more): [Assignment: organization-defined frequency]; when [Assignment: organization-defined configuration change conditions]].	1. Is this control applicable for the information system? 2. Is there a change control process in place for this information system? 3. The change control process includes which of the following? 4. Before changes are applied to the operational system, which of the following are completed?
CM-03(2)	Configuration Change Control | Testing, Validation, and Documentation of Changes	Test, validate, and document changes to the system before finalizing the implementation of the changes.	1. Is this control applicable for the information system? 2. Are system changes tested, validated, and documented before finalizing the implementation changes?
CM-03(4)	Configuration Change Control | Security and Privacy Representatives	Require [Assignment: organization-defined security and privacy representatives] to be members of the [Assignment: organization-defined configuration change control element].	1. Is this control applicable for the information system? 2. Is security and privacy representatives apart of the change control approval process?
CM-04	Impact Analyses	Analyze changes to the system to determine potential security and privacy impacts prior to change implementation.	1. Is this control applicable for the information system? 2. Does the organization perform security impact analysis prior to implementation?

CM-04(2)	Impact Analyses | Verification of Controls	After system changes, verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security and privacy requirements for the system.	1. Is this control applicable for the information system? 2. After system changes are implemented, are the impacted controls assessed with the desirable outcomes?
CM-05	Access Restrictions for Change	Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.	1. Is this control applicable for the information system? 2. Are configuration changes protected by physical and logical access restrictions? 3. Which of the following Access Restrictions to Change processes are implemented?
CM-06	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.	1. Is this control applicable for the information system? 2. Does the organization establish configuration settings for this information system and its components? 3. Are configuration settings configured with the most restrictive possible to meet requirements?

CM-07	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].	1. Is this control applicable for the information system? 2. Does the information system provide the least functionality to meet operational needs? 3. Does the information system prohibit or restrict ports, protocols, and services for all of the following areas: Software Systems? System Data? Systems Services? 4. Does the organization perform all of the following requirements: Review the information system to identify unnecessary and/or non-secure functions, ports, protocols, and services? Disable unnecessary or non-secure software systems access, data access, and system services? 5. Does the information system prevent program execution in accordance with the security plan?
CM-07(1)	Least Functionality | Periodic Review	(a) Review the system [Assignment: organization-defined frequency] to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services; and (b) Disable or remove [Assignment: organization-defined functions, ports, protocols, software, and services within the system deemed to be unnecessary and/or nonsecure].	1. Is this control applicable for the information system? 2. Does the information system periodically review nonsecure functions, ports, protocols, software, and services to identify those that are no longer needed? 3. Does the information system disable or remove nonsecure functions, ports, protocols, software, and services to identify those that are no longer needed?
CM-07(2)	Least Functionality | Prevent Program Execution	Prevent program execution in accordance with [Selection (one or more): [Assignment: organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions]; rules authorizing the terms and conditions of software program usage].	1. Is this control applicable for the information system? 2. Does the information system prevent program execution in accordance to policies and procedures?

CM-07(5)	Least Functionality | Authorized Software -- Allow by Exception	(a) Identify [Assignment: organization-defined software programs authorized to execute on the system]; (b) Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system; and (c) Review and update the list of authorized software programs [Assignment: organization-defined frequency].	1. Is this control applicable for the information system? 2. Does the organization perform all of the following requirements: Identify software programs not authorized to execute on the information system? Employ a deny-all, allow by exception policy to prohibit the execution of unauthorized software on the information system? Review and update a list of unauthorized software programs?
CM-08	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].	1. Is this control applicable for the information system? 2. Does the organization maintain an inventory of information system components? 3. Is system inventory documented such that all the following requirements are met: It accurately reflect the current information system? Includes all components within the authorization boundary? Is granular enough for tracking and reporting? Includes enough information, such as serial numbers and bar codes, to provide effective accountability? 4. Does the organization update the inventory whenever components are installed, removed, or updated? 5. Do you perform System Inventory Reviews? 6. The organization employs automated mechanisms to detect all of the following unauthorized device types: Hardware? Software? Firmware?
CM-08(1)	System Component Inventory | Updates During Installation and Removal	Update the inventory of system components as part of component installations, removals, and system updates.	1. Is this control applicable for the information system? 2. Is the inventory updated as a part of component installations, removals, and system updates?

CM-08(3)	System Component Inventory | Automated Unauthorized Component Detection	(a) Detect the presence of unauthorized hardware, software, and firmware components within the system using [Assignment: organization-defined automated mechanisms] [Assignment: organization-defined frequency]; and (b) Take the following actions when unauthorized components are detected: [Selection (one or more): disable network access by such components; isolate the components; notify [Assignment: organization-defined personnel or roles]].	1. Is this control applicable for the information system? 2. Are automated mechanisms in place to detect he presence of unauthorized hardware, software, and firmware components within the system? 3. Is an alert triggered to the IT staff when unauthorized components are detected?
CM-09	Configuration Management Plan	Control: Develop, document, and implement a configuration management plan for the system that: a. Addresses roles, responsibilities, and configuration management processes and procedures; b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items; c. Defines the configuration items for the system and places the configuration items under configuration management; d. Is reviewed and approved by [Assignment: organization-defined personnel or roles]; and e. Protects the configuration management plan from unauthorized disclosure and modification.	1. Is this control applicable for the information system? 2. Is there a configuration management plan for this information system? 3. Which of the following requirements does the configuration management plan address?
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.	1. Is this control applicable for the information system? 2. Does the organization have software usage restrictions?

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].	1. Is this control applicable for the information system? 2. Does the organization control user-installed software? 3. Is user-installed software controlled by organization defined policies? 4. Are those policies enforced through defined procedures and methods? 5. Is user-installed software monitored?
CM-12	Information Location	a. Identify and document the location of [Assignment: organization-defined information] and the specific system components on which the information is processed and stored; b. Identify and document the users who have access to the system and system components where the information is processed and stored; and c. Document changes to the location (i.e., system or system components) where the information is processed and stored.	1. Is this control applicable for the information system? 2. Has the location of system components on which PII is processed and stored been documented? 3. Have the users that have access to the system and system components where the information is processed and stored been documented?
CM-12(1)	Information Location | Automated Tools to Support Information Location	Use automated tools to identify [Assignment: organization-defined information by information type] on [Assignment: organization-defined system components] to ensure controls are in place to protect organizational information and individual privacy.	1. Is this control applicable for the information system? 2. are automated mechanisms in place to ensure controls are in place to protect organizational information and individual privacy?

CP-01	(Contingency Planning) 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].	1. Is this control applicable for the information system? 2. Is there a contingency planning policy? 3. Does the contingency plan policy address all of the following requirements? (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

CP-02	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.	1. Is this control applicable for the information system? 2. Is there a contingency plan for this information system? 3. Which of the following requirements does the contingency plan address? a. Identifies essential mission and business functions and associated contingency requirements; b. Provides recovery objectives, restoration priorities, and metrics; c. Addresses contingency roles, responsibilities, assigned individuals with contact information; d. Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure; e. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented; f. Addresses the sharing of contingency information; and g. Is reviewed and approved by [Assignment: organization-defined personnel or roles]; 4. Is the Contingency Plan distributed and communicated to Contingency Personnel and Senior Organization Officials?

CP-02(1)	Contingency Plan | Coordinate With Related Plans	Coordinate contingency plan development with organizational elements responsible for related plans.	1. Is this control applicable for the information system? 2. Does the system coordinate contingency plan development with organizational elements responsible for related plans?
CP-02(3)	Contingency Plan | Resume Mission and Business Functions	Plan for the resumption of [Selection: all; essential] mission and business functions within [Assignment: organization-defined time period] of contingency plan activation.	1. Is this control applicable for the information system? 2. Does the system plan for system resumption within organizational policy and procedure time frames?
CP-02(8)	Contingency Plan | Identify Critical Assets	Identify critical system assets supporting [Selection: all; essential] mission and business functions.	1. Is this control applicable for the information system? 2. The organization identifies critical information system assets supporting essential missions and business functions?
CP-03	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].	1. Is this control applicable for the information system? 2. Do you provide contingency training to contingency personnel consistent with assigned roles and responsibilities? 3. Do you provide training annually to the contingency personnel as a refresher?
CP-04	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.	1. Is this control applicable for the information system? 2. Do you perform contingency plan or disaster recovery testing to test the execution of the contingency plan? 3. Is the contingency plan or disaster recovery test conducted annually?

CP-04(1)	Contingency Plan Testing | Coordinate With Related Plans	Coordinate contingency plan testing with organizational elements responsible for related plans.	1. Is this control applicable for the information system? 2. Does the information system coordinate contingency plan testing with organizational elements responsible for related plans?
CP-06	Alternate Storage Site	a. Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information; and b. Ensure that the alternate storage site provides controls equivalent to that of the primary site.	1. Is this control applicable for the information system? 2. Do you use an alternate storage site specifically to store and retrieve system backups? 3. Is the alternate storage site required to, and meet, the same standard of security as the primary facility?
CP-06(1)	Alternate Storage Site | Separation From Primary Site	Identify an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats.	1. Is this control applicable for the information system? 2. Do you use an alternate storage site specifically to store and retrieve system backups?
CP-06(3)	Alternate Storage Site | Accessibility	Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.	1. Is this control applicable for the information system? 2. Have potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions been identified?
CP-07	Alternate Processing Site	a. Establish an alternate processing site, including necessary agreements to permit the transfer and resumption of [Assignment: organization-defined system operations] for essential mission and business functions within [Assignment: organization-defined time period consistent with recovery time and recovery point objectives] when the primary processing capabilities are unavailable; b. Make available at the alternate processing site, the equipment and supplies required to transfer and resume operations or put contracts in place to support delivery to the site within the organization-defined time period for transfer and resumption; and c. Provide controls at the alternate processing site that are equivalent to those at the primary site.	1. Is this control applicable for the information system? 2. Do you use an alternate processing site specifically to resume core business functions in the event of a disruption to the primary site? 3. Is the alternate processing site required to, and meet, the same standard of security as the primary facility?

CP-07(1)	Alternate Processing Site | Separation From Primary Site	Identify an alternate processing site that is sufficiently separated from the primary processing site to reduce susceptibility to the same threats.	1. Is this control applicable for the information system? 2. Is the alternate processing site sufficiently separated from the primary processing site to reduce susceptibility to the same threats?
CP-07(2)	Alternate Processing Site | Accessibility	Identify potential accessibility problems to alternate processing sites in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.	1. Is this control applicable for the information system? 2. Is the alternate processing site located separate from the primary site, in the case of a disaster?
CP-07(3)	Alternate Processing Site | Priority of Service	Develop alternate processing site agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives).	1. Is this control applicable for the information system? 2. Have alternate processing site agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives) been developed?
CP-08	Telecommunications Services	Establish alternate telecommunications services, including necessary agreements to permit the resumption of [Assignment: organization-defined system operations] for essential mission and business functions within [Assignment: organization-defined time period] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.	1. Is this control applicable for the information system? 2. Has your organization established an alternate telecommunications services for the alternate processing site with the necessary agreements to permit the resumption of core missions and business functions?
CP-08(1)	Telecommunications Services | Priority of Service Provisions	(a) Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives); and (b) Request Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness if the primary and/or alternate telecommunications services are provided by a common carrier.	1. Is this control applicable for the information system? 2. Have telecommunication service agreements been created to include the following? (a)Contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives); and (b) Request Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness if the primary and/or alternate telecommunications services are provided by a common carrier.

CP-08(2)	Telecommunications Services | Single Points of Failure	Obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.	1. Is this control applicable for the information system? 2. Have alternate telecommunications services been established to reduce the likelihood of sharing a single point of failure with primary telecommunications services?
CP-09	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.	1. Is this control applicable for the information system? 2. Does your organization conduct backups of all information system information? 3. Does your organization conduct backups of user-level information contained in the information system? 4. Does your organization conduct backups of system-level information contained in the information system? 5. Does your organization conduct backups of information system documentation including security-related documentation? 6. Do you protect the confidentiality, integrity, and availability of backup information at storage locations?
CP-09(1)	System Backup | Testing for Reliability and Integrity	Test backup information [Assignment: organization-defined frequency] to verify media reliability and information integrity.	1. Is this control applicable for the information system? 2. Do you tests backup information to verify media reliability and information integrity?
CP-09(8)	System Backup | Cryptographic Protection	Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of [Assignment: organization-defined backup information].	1. Is this control applicable for the information system? Have cryptographic mechanisms been put in place on system backups to prevent unauthorized disclosure and modification?

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.	1. Is this control applicable for the information system? 2. Does your organization provide recovery and reconstitution procedures for primary facility to bring the facility back to a known state after a disruption, compromise, or failure?
CP-10(2)	System Recovery and Reconstitution | Transaction Recovery	Implement transaction recovery for systems that are transaction-based.	Not applicable to GAs
IA-01	(Identification and Authentication) 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].	1.Is this control applicable for the information system? 2.Has an identification and authentication policy and procedures which cover all information systems within the security boundary been developed and disseminated to all employees? 3. Does the policy address the following requirements: (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 4. Do the procedures facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls and designate an officials to manage the development, documentation, and dissemination of the identification and authentication policy and procedures? 5. What is the frequency that the policies and procedures are reviewed and updated, if needed, by management?

IA-02	Identification and Authentication (Organizational Users)	Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.	1. Is this control applicable for the information system? 2. For each information system within the security boundary, are organizational users uniquely identified and authenticated?
IA-02(1)	Identification and Authentication (Organizational Users) | Multifactor Authentication to Privileged Accounts	Implement multi-factor authentication for access to privileged accounts.	1. Is this control applicable for the information system? 2. For each information system within the security boundary, are privileged users required to authenticate using multi-factor authentication?
IA-02(12)	Identification and Authentication (Organizational Users) | Acceptance of PIV Credentials	Accept and electronically verify Personal Identity Verification-compliant credentials.	1. Is this control applicable for the information system? 2. Are Personal Identity Verification-compliant credentials in place?
IA-02(2)	Identification and Authentication (Organizational Users) | Multifactor Authentication to Non-Privileged Accounts	Implement multi-factor authentication for access to non-privileged accounts.	1. Is this control applicable for the information system? 2. For each information system within the security boundary, are non-privileged users required to authenticate using multi-factor authentication?
IA-02(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].	1. Is this control applicable for the information system? 2. Are replay-resistant authentication mechanisms in place?
IA-03	Device Identification and Authentication	Uniquely identify and authenticate [Assignment: organization-defined devices and/or types of devices] before establishing a [Selection (one or more): local; remote; network] connection.	1. Is this control applicable for the information system? 2. For each information system within the security boundary, are devices uniquely identified and require authentication mechanisms before establishing a network connection?

IA-04	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].	1. Is this control applicable for the information system? 2. For each information system within the security boundary, are approvals required prior to assigning an individual, group, role or device and identifier? 3. For each information system within the security boundary, are identifiers ever re-used? 4. For each information system within the security boundary, are identifiers disabled when no longer in use?
IA-04(4)	Identifier Management | Identify User Status	Manage individual identifiers by uniquely identifying each individual as [Assignment: organization-defined characteristic identifying individual status].	1. Is this control applicable for the information system? 2. Does each unique identifier have an associated status (e.g., disabled or enabled)?

IA-05	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.	1. Is this control applicable for the information system? 2. For each information system within the security boundary, are authenticators managed by all of the following parameters: a) Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role or device receiving the authenticator b) Establishing initial authenticator content for authenticators defined by the organization c) Ensuring that authenticators have sufficient strength of mechanism for their intended use? 3. For each information system within the security boundary, which parameters manage all authenticators? 4. For each information system within the security boundary that uses password-based authentication, the information system enforces a minimum password complexity of? 5. For each information system within the security boundary that uses password-based authentication, does the information system enforces at least a number of changed characters when new passwords are created? 6. For each information system within the security boundary that uses password-based authentication, does the information system stores and transmits only encrypted representations of passwords?

IA-05(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].	1. Is this control applicable for the information system? 2. Does the following occur 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) Enforcement of complexity rules
IA-05(2)	Authenticator Management | Public Key-Based Authentication	(a) For public key-based authentication: (1) Enforce authorized access to the corresponding private key; and (2) Map the authenticated identity to the account of the individual or group; and (b) When public key infrastructure (PKI) is used: (1) Validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information; and (2) Implement a local cache of revocation data to support path discovery and validation.	1. Is this control applicable for the information system? 2. Does the following occur for public key based authentication: (a) Enforce authorized access to the corresponding private key; and (b) Map the authenticated identity to the account of the individual or group;

IA-05(6)	Authenticator Management | Protection of Authenticators	Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access.	1. Is this control applicable for the information system? 2. Are authenticators protected with the security category of the information to which use of the authenticator permits access?
IA-06	Authenticator Feedback	Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.	1. Is this control applicable for the information system? 2. For each information system within the security boundary, does the information system obscure feedback of authentication information during the authentication process?
IA-07	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.	1. Is this control applicable for the information system? 2. For each information system within the security boundary, does the information system implement mechanisms for authentication to a cryptographic module that meets the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication?
IA-08	Identification and Authentication (Non-Organizational Users)	Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.	1. Is this control applicable for the information system? 2. For each information system within the security boundary, does the information system uniquely identify and authenticate non-organizational users (or processes acting on behalf of non-organizational users)?
IA-08(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.	Not applicable to GAs
IA-08(2)	Identification and Authentication (Non-Organizational Users) | Acceptance of External Party Credentials	(a) Accept only external authenticators that are NIST-compliant; and (b) Document and maintain a list of accepted external authenticators.	1. Is this control applicable for the information system? 2. Are only external authenticators that are NIST-compliant accepted? 3. Are a list of acceptable external authenticators documented and maintained?

IA-08(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].	1. Is this control applicable for the information system? 2. Have user profiles been defined?
IA-11	Re-Authentication	Require users to re-authenticate when [Assignment: organization-defined circumstances or situations requiring re-authentication].	1. Is this control applicable for the information system? 2. Are users required to re-authenticate after 15 minutes of inactivity?
IA-12	Identity Proofing	a. Identity proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines; b. Resolve user identities to a unique individual; and c. Collect, validate, and verify identity evidence.	1. Is this control applicable for the information system? 2. Is proof of identity required for accounts logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines? 2. Are user identities resolved to a unique individual? 3. Is identity evidence collected, validated, and verified?
IA-12(2)	Identity Proofing | Identity Evidence	Require evidence of individual identification be presented to the registration authority.	1. Is this control applicable for the information system? 2. Is evidence of individual identification required to be presented to the registration authority?
IA-12(3)	Identity Proofing | Identity Evidence Validation and Verification	Require that the presented identity evidence be validated and verified through [Assignment: organizational defined methods of validation and verification].	1. Is this control applicable for the information system? 2. Is identity evidence validated?
IA-12(5)	Identity Proofing | Address Confirmation	Require that a [Selection: registration code; notice of proofing] be delivered through an out-of-band channel to verify the users address (physical or digital) of record.	1. Is this control applicable for the information system? 2. Is a notice sent through an out-of-band channel to verify the users address (physical or digital) of record?

IR-01	(Incident Response) 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].	1. Is this control applicable for the information system? 2. Is there an incident response policy? 3. Does the incidence response policy address the following? (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; 4. Is the incident response policy updated annually? 5. Are there procedures for incident response planning? 6. Is there a designated official to manage the development, documentation, and dissemination of the incident response policy and procedures? 7. Are the procedures for incidence response updated annually?
IR-02	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].	1. Is this control applicable for the information system? 2. Is there incident response training for users with assigned contingency roles? 3. For which timeframes does incident response training occur?

IR-02(3)	Incident Response Training | Breach	Provide incident response training on how to identify and respond to a breach, including the organization's process for reporting a breach.	1. Is this control applicable for the information system? 2. Is training provided on how to identify and respond to a breach?
IR-03	Incident Response Testing	Test the effectiveness of the incident response capability for the system [Assignment: organization-defined frequency] using the following tests: [Assignment: organization-defined tests].	1. Is this control applicable for the information system? 2. Is the incident response capability tested? 3. For which requirements is the contingency plan tested and documented?
IR-03(2)	Incident Response Testing | Coordination With Related Plans	Coordinate incident response testing with organizational elements responsible for related plans.	1. Is this control applicable for the information system? 2. Incident response testing coordinated with organizational elements responsible for related plans?
IR-04	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.	1. Is this control applicable for the information system? 2. Does the organization implement an incident response capability? 3. For which of the following is the incident response capability performed: (a)Rigor, (b) intensity, (c) scope, and (d)results of incident handling activities are comparable and predictable across the organization.
IR-04(1)	Incident Handling | Automated Incident Handling Processes	Support the incident handling process using [Assignment: organization-defined automated mechanisms].	1. Is this control applicable for the information system? 2. Are automated mechanisms in placed to support the incident response?
IR-05	Incident Monitoring	Track and document incidents.	1. Is this control applicable for the information system? 2. Are incidents tracked and documented?

IR-06	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].	1. Is this control applicable for the information system? 2. Are security incidents reported?
IR-06(1)	Incident Reporting | Automated Reporting	Report incidents using [Assignment: organization-defined automated mechanisms].	1. Is this control applicable for the information system? 2. Do automated mechanisms support security incident reporting?
IR-06(3)	Incident Reporting | Supply Chain Coordination	Provide incident information to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident.	1. Is this control applicable for the information system? 2. Is incident information provided to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident?
IR-07	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.	1. Is this control applicable for the information system? 2. Is there an incident response support resource?
IR-07(1)	Incident Response Assistance | Automation Support for Availability of Information and Support	Increase the availability of incident response information and support using [Assignment: organization-defined automated mechanisms].	1. Is this control applicable for the information system? 2. Are there automated mechanisms to increase the availability of incident response information?

IR-08	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.	1. Is this control applicable for the information system? 2. Is there an incident response plan? 3. Which of the following does the incident response plan describe: a. Provides the organization with a roadmap for implementing its incident response capability; b. Describes the structure and organization of the incident response capability; c. Provides a high-level approach for how the incident response capability fits into the overall organization; d. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; e. Defines reportable incidents; f. Provides metrics for measuring the incident response capability within the organization; g. Defines the resources and management support needed to effectively maintain and mature an incident response capability; h. Addresses the sharing of incident information; i. Is reviewed and approved annually; and j. Explicitly designates responsibility for incident response to [Assignment: organization-defined entities, personnel, or roles].

IR-08(1)	Incident Response Plan | Breaches	Include the following in the Incident Response Plan for breaches involving personally identifiable information: (a) A process to determine if notice to individuals or other organizations, including oversight organizations, is needed; (b) An assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms; and (c) Identification of applicable privacy requirements.	1. Is this control applicable for the information system? 2. Has an incident response plan for breaches been created to include the following: (a) A process to determine if notice to individuals or other organizations, including oversight organizations, is needed; (b) An assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms; and (c) Identification of applicable privacy requirements.
MA-01	(Maintenance) 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].	1. Is this control applicable for the information system? 2. Is there a system 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 3. Is the system maintenance policy disseminated to Information technology personnel and executive management? 4. Is the system maintenance policy reviewed and updated annually? 5. Are there procedures in place to facilitate the implementation of the system maintenance policy and associated system maintenance controls? 6. Has a designated official been assigned to manage the development, documentation, and dissemination of the maintenance policy and procedures? 7. Are the system maintenance procedures reviewed and updated annually?

MA-02	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].	1. Is this control applicable for the information system? 2. Are maintenance and repairs on information system components meeting all the following requirements: i) Scheduled ii) Performed iii) Documented iv) Records reviewed in accordance with manufacturer or vendor specifications and/or organization requirements? 3. Are all maintenance activities approved and monitored, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location? 4. Do the Chief Information Officer and Technology Officer explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs?
MA-03	Maintenance Tools	a. Approve, control, and monitor the use of system maintenance tools; and b. Review previously approved system maintenance tools [Assignment: organization-defined frequency].	1. Is this control applicable for the information system? 2. Are information system maintenance tools following all the procedures below: i) Approved ii) Controlled iii) Monitored?
MA-03(1)	Maintenance Tools | Inspect Tools	Inspect the maintenance tools used by maintenance personnel for improper or unauthorized modifications.	1. Is this control applicable for the information system? 2. Are maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modification inspected?
MA-03(2)	Maintenance Tools | Inspect Media	Check media containing diagnostic and test programs for malicious code before the media are used in the system.	1. Is this control applicable for the information system? 2. Are media containing diagnostic and test programs for malicious code checked before the media are used in the information system?

MA-03(3)	Maintenance Tools | Prevent Unauthorized Removal	Prevent the removal of maintenance equipment containing organizational information by: (a) Verifying that there is no organizational information contained on the equipment; (b) Sanitizing or destroying the equipment; (c) Retaining the equipment within the facility; or (d) Obtaining an exemption from [Assignment: organization-defined personnel or roles] explicitly authorizing removal of the equipment from the facility.	1. Is this control applicable for the information system? 2. Is the removal of organizational maintenance equipment prevented by (a) Verifying that there is no organizational information contained on the equipment; (b) Sanitizing or destroying the equipment; (c) Retaining the equipment within the facility; or (d) Obtaining an exemption to explicitly authorizing removal of the equipment from the facility.
MA-04	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.	1. Is this control applicable for the information system? 2. Are nonlocal maintenance and diagnostic activities following all the procedures below: i) Approved ii) Monitored? 3. Is the use of nonlocal maintenance and diagnostic tools allowed only as consistent with organizational policy and documented in the security plan for the information system? 4. Are strong authenticators employed in the establishment of nonlocal maintenance and diagnostic sessions? 5. Are records maintained for nonlocal maintenance and diagnostic activities?
MA-05	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.	1. Is this control applicable for the information system? 2. Is there a process for maintenance personnel authorization? 3. Is a list of authorized maintenance organizations or personnel maintained? 4. Do non-escorted personnel performing maintenance on the information system have required access authorizations? 5. Are organizational personnel with required access authorizations and technical competence designated to supervise the maintenance activities of personnel who do not possess the required access authorizations?

MA-06	Timely Maintenance	Obtain maintenance support and/or spare parts for [Assignment: organization-defined system components] within [Assignment: organization-defined time period] of failure.	1. Is this control applicable for the information system? 2. Is maintenance support and/or spare parts for all hardware obtained within 72 hours (or less) of failure?
MP-01	(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].	1. Is this control applicable for the information system? 2. Is there a media protection policy that addresses the following: (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 3. Is the media protection policy disseminated to the appropriate stakeholders? 4. Is the media protection policy reviewed and updated annually? 5. Are there procedures in place to facilitate the implementation of the media protection policy and associated media protection controls? 6. Has an official been designated to manage the development, documentation, and dissemination of the media protection policy and procedures? 7. Are the media protection procedures reviewed and updated annually?
MP-02	Media Access	Restrict access to [Assignment: organization-defined types of digital and/or non-digital media] to [Assignment: organization-defined personnel or roles].	1. Is this control applicable for the information system? 2. Does the organization restrict access to digital and physical media to only authorized personnel?

MP-03	Media Marking	a. Mark system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and b. Exempt [Assignment: organization-defined types of system media] from marking if the media remain within [Assignment: organization-defined controlled areas].	1. Is this control applicable for the information system? 2. Does the organization mark physical media indicating the distribution limitations, handling caveats, and applicable security markings?
MP-04	Media Storage	a. Physically control and securely store [Assignment: organization-defined types of digital and/or non-digital media] within [Assignment: organization-defined controlled areas]; and b. Protect system media types defined in MP-4a until the media are destroyed or sanitized using approved equipment, techniques, and procedures.	1. Is this control applicable for the information system? 2. Are media stored secured at all times when in storage and are there physical controls in place to protect media from unauthorized use or disclosure?
MP-05	Media Transport	a. Protect and control [Assignment: organization-defined types of system media] during transport outside of controlled areas using [Assignment: organization-defined controls]; b. Maintain accountability for system media during transport outside of controlled areas; c. Document activities associated with the transport of system media; and d. Restrict the activities associated with the transport of system media to authorized personnel.	1. Is this control applicable for the information system? 2. Are there security policies and requirements around the protection of media in storage and in transit to other facilities? 3. Are there security policies and requirements around the protection of media in storage and in transit to other facilities?
MP-06	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.	1. Is this control applicable for the information system? 2. Are all digital media sanitized prior to disposal, release for reuse, or release outside of the organization?

MP-07	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.	1. Is this control applicable for the information system? 2. Does the organization of a "Media Usage" and "Media Restriction" policy in place that defines what digital media can be used, by whom and where?
PE-01	(Physical and Environmental 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] 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].	UPDATE: Is there a physical and environmental protection policy? ADD ON: Select one or more of the following that best describes the policy: Organization-level; Mission/business process-level; System-level UPDATE: Which of the following requirements are addressed by the physical and environmental protection policy? ADD ON: IS consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines ADD: Has an organization-defined official designated to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures?

PE-02	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	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.	ADD: Are individual access authorizations verified before granting access to the facility? ADD: How is ingress and egress to the facility controlled? Select all that apply: organization-defined physical access control systems or devices, guards, other. ADD: Are physical access audit logs for entry and exit points maintained? ADD: Are physical access controls implemented to control areas within the facility designated as publicly accessible? ADD: Are there defined circumstances requiring visitor escorts and control of visitor activity? (Can provide further detail in the Comment Box) ADD: Are keys, combinations, and other physical access devices secured? ADD: Are physical access devices for the organization inventoried? ADD: If yes, how often are the devices inventoried? Annually, Biennially (every 2 years), Triennially, other. ADD: Are combinations and keys changed when keys are lost, combinations are compromised, individuals possessing the keys or combinations are transferred or terminated, or at a set frequency.

PE-04	Access Control for Transmission	Control physical access to [Assignment: organization-defined system distribution and transmission lines] within organizational facilities using [Assignment: organization-defined security controls].	
PE-05	Access Control for Output Devices	Control physical access to output from [Assignment: organization-defined output devices] to prevent unauthorized individuals from obtaining the output.	
PE-06	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-06(1)	Monitoring Physical Access | Intrusion Alarms and Surveillance Equipment	Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment.	
PE-08	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-08(3)	Visitor Access Records | Limit Personally Identifiable Information Elements	Limit personally identifiable information contained in visitor access records to the following elements identified in the privacy risk assessment: [Assignment: organization-defined elements].	Is personally identifiable information (PII) contained in visitor access records limited to the following elements identified in the privacy risk assessment?

PE-09	Power Equipment and Cabling	Protect power equipment and power cabling for the system from damage and destruction.	
PE-10	Emergency Shutoff	a. Provide the capability of shutting off power to [Assignment: organization-defined system or individual system components] in emergency situations; b. Place emergency shutoff switches or devices in [Assignment: organization-defined location by system or system component] to facilitate access for authorized personnel; and c. Protect emergency power shutoff capability from unauthorized activation.	
PE-11	Emergency Power	Provide an uninterruptible power supply to facilitate [Selection (one or more): an orderly shutdown of the system; transition of the system to long-term alternate power] in the event of a primary power source loss.	Is the selected control baseline tailored by applying specified tailoring actions.
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	Fire Protection	Employ and maintain fire detection and suppression systems that are supported by an independent energy source.	
PE-13(1)	Fire Protection | Detection Systems – Automatic Activation and Notification	Employ fire detection systems that activate automatically and notify [Assignment: organization-defined personnel or roles] and [Assignment: organization-defined emergency responders] in the event of a fire.	Has an inventory of all systems, applications, and projects that process personally identifiable information (PII) been i) established, ii) maintained, and iii) updated? If yes, is that inventory reviewed and updated at least annually?

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	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	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	Alternate Work Site	a. Determine and document the [Assignment: organization-defined alternate work sites] allowed for use by employees; b. Employ the following controls at alternate work sites: [Assignment: organization-defined controls]; c. Assess the effectiveness of controls at alternate work sites; and d. Provide a means for employees to communicate with information security and privacy personnel in case of incidents.	

PL-01	(Planning) 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	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	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(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	Security and Privacy Architectures	a. Develop security and privacy architectures for the system that: 1. Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information; 2. Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals; 3. Describe how the architectures are integrated into and support the enterprise architecture; and 4. Describe any assumptions about, and dependencies on, external systems and services; b. Review and update the architectures [Assignment: organization-defined frequency] to reflect changes in the enterprise architecture; and c. Reflect planned architecture changes in security and privacy plans, Concept of Operations (CONOPS), criticality analysis, organizational procedures, and procurements and acquisitions.	Is there a policy and procedures established to ensure protection of controlled unclassified information on external systems? If yes, is the policy and procedures review and updated at least annually?

PL-09	Central Management	Centrally manage [Assignment: organization-defined controls and related processes].	Has an organization-wide privacy plan been developed and disseminated that provides an overview of the agency's privacy program? Does the plan include the following? Select all that apply: a) Description of the structure of the privacy program and the resources dedicated to the privacy program; b) An overview of the requirements for the privacy program and a description of the privacy program management controls and common controls in place or planned for meeting those requirements; c) The role of the senior agency official for privacy and the identification and assignment of roles of other privacy officials and staff and their responsibilities; d) Description of management commitment, compliance, and the strategic goals and objectives of the privacy program; e) Reflects coordination among organizational entities responsible for the different aspects of privacy; and f) Is approved by a senior official with responsibility and accountability for the privacy risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation. Is the plan updated at least annually and to address changes in federal privacy laws and policy and organizational changes and problems identified during plan implementation or privacy control assessments?
PL-10	Baseline Selection	Select a control baseline for the system.	Has a senior agency official been appointed for privacy with the authority, mission, accountability, and resources to coordinate, develop, and implement, applicable privacy requirements and manage privacy risks through the organization-wide privacy program.

PL-11	Baseline Tailoring	Tailor the selected control baseline by applying specified tailoring actions.	Is there a central resource webpage maintained on the organization's principal public website that serves as a central source of information about the organization's privacy program? If yes, select all that apply to the webpage: a) Ensures that the public has access to information about organizational privacy activities and can communicate with its senior agency official for privacy; b) Ensures that organizational privacy practices and reports are publicly available; and c) Employs publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to privacy offices regarding privacy practices.
PM-03	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.	Are privacy policies posted on all external-facing websites, mobile applications, and other digital services? If yes, select all that apply to the policies: a) Written in plain language and organized in a way that is easy to understand and navigate; b) Provide information needed by the public to make an informed decision about whether and how to interact with the organization; and c) Updated whenever the organization makes a substantive change to the practices it describes and includes a time/date stamp to inform the public of the date of the most recent changes.

PM-04	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.	Has an accurate accounting of disclosures of personally identifiable information (PII) been developed and maintained. If yes, select all that apply to the accounting: a) Date, nature, and purpose of each disclosure; b) Name and address, or other contact information of the individual or organization to which the disclosure was made How long are the accounting of disclosures retained? a) For the length of the time the PII is maintained, b) Five years after the disclosure is made, c) Whichever is longer, d) Other. Upon request, are the accounting of disclosures made available to the individual to whom the PII relates?
PM-05(1)	System Inventory | Inventory of Personally Identifiable Information	Establish, maintain, and update [Assignment: organization-defined frequency] an inventory of all systems, applications, and projects that process personally identifiable information.	Has an inventory of all systems, applications, and projects that process personally identifiable information (PII) been i) established, ii) maintained, and iii) updated? If yes, is that inventory reviewed and updated at least annually?
PM-06	Measures of Performance	Develop, monitor, and report on the results of information security and privacy measures of performance.	
PM-07	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	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	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	
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	
PM-11	Mission and 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	
PM-13	Security and Privacy Workforce	Establish a security and privacy workforce development and improvement program.	
PM-14	Testing, Training, and Monitoring	a. Implement a process for ensuring that organizational plans for conducting security and privacy testing, training, and monitoring activities associated with organizational systems: 1. Are developed and maintained; and 2. Continue to be executed; and b. Review testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.	
PM-17	Protecting Controlled Unclassified Information On External Systems	a. Establish policy and procedures to ensure that requirements for the protection of controlled unclassified information that is processed, stored or transmitted on external systems, are implemented in accordance with applicable laws, executive orders, directives, policies, regulations, and standards; and b. Review and update the policy and procedures [Assignment: organization-defined frequency].	Is there a policy and procedures established to ensure protection of controlled unclassified information on external systems? If yes, is the policy and procedures review and updated at least annually?

PM-18	Privacy Program Plan	a. Develop and disseminate an organization-wide privacy program plan that provides an overview of the agency's privacy program, and: 1. Includes a description of the structure of the privacy program and the resources dedicated to the privacy program; 2. Provides an overview of the requirements for the privacy program and a description of the privacy program management controls and common controls in place or planned for meeting those requirements; 3. Includes the role of the senior agency official for privacy and the identification and assignment of roles of other privacy officials and staff and their responsibilities; 4. Describes management commitment, compliance, and the strategic goals and objectives of the privacy program; 5. Reflects coordination among organizational entities responsible for the different aspects of privacy; and 6. Is approved by a senior official with responsibility and accountability for the privacy risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; and b. Update the plan [Assignment: organization-defined frequency] and to address changes in federal privacy laws and policy and organizational changes and problems identified during plan implementation or privacy control assessments.	Has an organization-wide privacy plan been developed and disseminated that provides an overview of the agency's privacy program? Does the plan include the following? Select all that apply: a) Description of the structure of the privacy program and the resources dedicated to the privacy program; b) An overview of the requirements for the privacy program and a description of the privacy program management controls and common controls in place or planned for meeting those requirements; c) The role of the senior agency official for privacy and the identification and assignment of roles of other privacy officials and staff and their responsibilities; d) Description of management commitment, compliance, and the strategic goals and objectives of the privacy program; e) Reflects coordination among organizational entities responsible for the different aspects of privacy; and f) Is approved by a senior official with responsibility and accountability for the privacy risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation. Is the plan updated at least annually and to address changes in federal privacy laws and policy and organizational changes and problems identified during plan implementation or privacy control assessments?
PM-19	Privacy Program Leadership Role	Appoint a senior agency official for privacy with the authority, mission, accountability, and resources to coordinate, develop, and implement, applicable privacy requirements and manage privacy risks through the organization-wide privacy program.	Has a senior agency official been appointed for privacy with the authority, mission, accountability, and resources to coordinate, develop, and implement, applicable privacy requirements and manage privacy risks through the organization-wide privacy program.

PM-20	Dissemination of Privacy Program Information	Maintain a central resource webpage on the organization's principal public website that serves as a central source of information about the organization's privacy program and that: a. Ensures that the public has access to information about organizational privacy activities and can communicate with its senior agency official for privacy; b. Ensures that organizational privacy practices and reports are publicly available; and c. Employs publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to privacy offices regarding privacy practices.	Is there a central resource webpage maintained on the organization's principal public website that serves as a central source of information about the organization's privacy program? If yes, select all that apply to the webpage: a) Ensures that the public has access to information about organizational privacy activities and can communicate with its senior agency official for privacy; b) Ensures that organizational privacy practices and reports are publicly available; and c) Employs publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to privacy offices regarding privacy practices.
PM-20(1)	Dissemination of Privacy Program Information | Privacy Policies on Websites, Applications, and Digital Services	Develop and post privacy policies on all external-facing websites, mobile applications, and other digital services, that: (a) Are written in plain language and organized in a way that is easy to understand and navigate; (b) Provide information needed by the public to make an informed decision about whether and how to interact with the organization; and (c) Are updated whenever the organization makes a substantive change to the practices it describes and includes a time/date stamp to inform the public of the date of the most recent changes.	Are privacy policies posted on all external-facing websites, mobile applications, and other digital services? If yes, select all that apply to the policies: a) Written in plain language and organized in a way that is easy to understand and navigate; b) Provide information needed by the public to make an informed decision about whether and how to interact with the organization; and c) Updated whenever the organization makes a substantive change to the practices it describes and includes a time/date stamp to inform the public of the date of the most recent changes.

PM-21	Accounting of Disclosures	a. Develop and maintain an accurate accounting of disclosures of personally identifiable information, including: 1. Date, nature, and purpose of each disclosure; and 2. Name and address, or other contact information of the individual or organization to which the disclosure was made; b. Retain the accounting of disclosures for the length of the time the personally identifiable information is maintained or five years after the disclosure is made, whichever is longer; and c. Make the accounting of disclosures available to the individual to whom the personally identifiable information relates upon request.	Has an accurate accounting of disclosures of personally identifiable information (PII) been developed and maintained. If yes, select all that apply to the accounting: a) Date, nature, and purpose of each disclosure; b) Name and address, or other contact information of the individual or organization to which the disclosure was made How long are the accounting of disclosures retained? a) For the length of the time the PII is maintained, b) Five years after the disclosure is made, c) Whichever is longer, d) Other. Upon request, are the accounting of disclosures made available to the individual to whom the PII relates?
PM-22	Personally Identifiable Information Quality Management	Develop and document organization-wide policies and procedures for: a. Reviewing for the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle; b. Correcting or deleting inaccurate or outdated personally identifiable information; c. Disseminating notice of corrected or deleted personally identifiable information to individuals or other appropriate entities; and d. Appeals of adverse decisions on correction or deletion requests.	Do you have organization-wide policies and procedures for the following, select all that apply: a. Reviewing for the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle; b. Correcting or deleting inaccurate or outdated personally identifiable information; c. Disseminating notice of corrected or deleted personally identifiable information to individuals or other appropriate entities; and d. Appeals of adverse decisions on correction or deletion requests.
PM-24	Data Integrity Board	Establish a Data Integrity Board to: a. Review proposals to conduct or participate in a matching program; and b. Conduct an annual review of all matching programs in which the agency has participated.	Has a Data Integrity Board been established? If yes, are the following tasks performed, select all that apply: a. Review proposals to conduct or participate in a matching program; and b. Conduct an annual review of all matching programs in which the agency has participated.

PM-25	Minimization of Personally Identifiable Information Used In Testing, Training, and Research	a. Develop, document, and implement policies and procedures that address the use of personally identifiable information for internal testing, training, and research; b. Limit or minimize the amount of personally identifiable information used for internal testing, training, and research purposes; c. Authorize the use of personally identifiable information when such information is required for internal testing, training, and research; and d. Review and update policies and procedures [Assignment: organization-defined frequency].	Have policies and procedures been developed, documented, and implemented? If yes, do they address the following? Select all that apply: a. The use of personally identifiable information (PII) for internal testing, training, and research; b. Limit or minimize the amount of personally identifiable information used for internal testing, training, and research purposes; c. Authorize the use of personally identifiable information when such information is required for internal testing, training, and research; and d. Review and update policies and procedures at an organization-defined frequency.
PM-26	Complaint Management	Implement a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational security and privacy practices that includes: a. Mechanisms that are easy to use and readily accessible by the public; b. All information necessary for successfully filing complaints; c. Tracking mechanisms to ensure all complaints received are reviewed and addressed within [Assignment: organization-defined time period]; d. Acknowledgement of receipt of complaints, concerns, or questions from individuals within [Assignment: organization-defined time period]; and e. Response to complaints, concerns, or questions from individuals within [Assignment: organization-defined time period].	Is there a process implemented for receiving and responding to complaints, concerns, or questions from individuals about the organizational security and privacy practices. If yes, does that process include the following? Select all that apply: a. Mechanisms that are easy to use and readily accessible by the public; b. All information necessary for successfully filing complaints; c. Tracking mechanisms to ensure all complaints received are reviewed and addressed within an organization-defined time period; d. Acknowledgement of receipt of complaints, concerns, or questions from individuals within an organization-defined time period; and e. Response to complaints, concerns, or questions from individuals within an organization-defined time period.

PM-27	Privacy Reporting	a. Develop [Assignment: organization-defined privacy reports] and disseminate to: 1. [Assignment: organization-defined oversight bodies] to demonstrate accountability with statutory, regulatory, and policy privacy mandates; and 2. [Assignment: organization-defined officials] and other personnel with responsibility for monitoring privacy program compliance; and b. Review and update privacy reports [Assignment: organization-defined frequency].	Has a privacy report(s) been developed? If yes, are the report(s): a) Disseminated to organization-defined oversight bodies to demonstrate accountability with statutory, regulatory, and policy privacy mandates and other personnel with responsibility for monitoring privacy program compliance b. Reviewed and updated at least annually.
PM-28	Risk Framing	a. Identify and document: 1. Assumptions affecting risk assessments, risk responses, and risk monitoring; 2. Constraints affecting risk assessments, risk responses, and risk monitoring; 3. Priorities and trade-offs considered by the organization for managing risk; and 4. Organizational risk tolerance; b. Distribute the results of risk framing activities to [Assignment: organization-defined personnel]; and c. Review and update risk framing considerations [Assignment: organization-defined frequency].	Are the following identified and documented? Select all that apply: 1. Assumptions affecting risk assessments, risk responses, and risk monitoring; 2. Constraints affecting risk assessments, risk responses, and risk monitoring; 3. Priorities and trade-offs considered by the organization for managing risk; and 4. Organizational risk tolerance; Are the results of risk framing activities distributed to organization-defined personnel? Are the risk framing considerations reviewed and updated at least annually?

PM-31	Continuous Monitoring Strategy	Develop an organization-wide continuous monitoring strategy and implement continuous monitoring programs that include: a. Establishing the following organization-wide metrics to be monitored: [Assignment: organization-defined metrics]; b. Establishing [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessment of control effectiveness; c. Ongoing monitoring of organizationally-defined metrics in accordance with the continuous monitoring strategy; d. Correlation and analysis of information generated by control assessments and monitoring; e. Response actions to address results of the analysis of control assessment and monitoring information; and f. Reporting the security and privacy status of organizational systems to [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency].	Has an organization-wide continuous monitoring strategy been developed and a continuous monitoring program implemented? If yes, have the following parameters been determined and implemented? Select all that apply: a. Establishing organization-wide metrics to be monitored b. Establishing organization-defined frequencies for monitoring and assessment of control effectiveness; c. Ongoing monitoring of organizationally-defined metrics in accordance with the continuous monitoring strategy; d. Correlation and analysis of information generated by control assessments and monitoring; e. Response actions to address results of the analysis of control assessment and monitoring information; and f. Reporting the security and privacy status of organizational systems to organization-defined personnel or roles at an organization-defined frequency.

PS-01	(Personnel Security) 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	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	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	Personnel Termination	Upon termination of individual employment: 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	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	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	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	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.	

PS-09	Position Descriptions	Incorporate security and privacy roles and responsibilities into organizational position descriptions.	Have security and privacy roles and responsibilities been implemented into organizational position descriptions?
PT-01	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] personally identifiable information processing and transparency 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 personally identifiable information processing and transparency policy and the associated personally identifiable information processing and transparency controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the personally identifiable information processing and transparency policy and procedures; and c. Review and update the current personally identifiable information processing and transparency: 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].	

PT-02	Authority to Process Personally Identifiable Information	a. Determine and document the [Assignment: organization-defined authority] that permits the [Assignment: organization-defined processing] of personally identifiable information; and b. Restrict the [Assignment: organization-defined processing] of personally identifiable information to only that which is authorized.	
PT-02(1)	Authority to Process Personally Identifiable Information | DATA TAGGING	Attach data tags containing [Assignment: organization-defined authorized processing] to [Assignment: organization-defined elements of personally identifiable information].	
PT-02(2)	Authority to Process Personally Identifiable Information | AUTOMATION	Manage enforcement of the authorized processing of personally identifiable information using [Assignment: organization-defined automated mechanisms].	

PT-03	Personally Identifiable Information Processing Purposes	Identify and document the [Assignment: organization-defined purpose(s)] for processing personally identifiable information; b. Describe the purpose(s) in the public privacy notices and policies of the organization; c. Restrict the [Assignment: organization-defined processing] of personally identifiable information to only that which is compatible with the identified purpose(s); and d. Monitor changes in processing personally identifiable information and implement [Assignment: organization-defined mechanisms] to ensure that any changes are made in accordance with [Assignment: organization-defined requirements].	
PT-03(1)	Personally Identifiable Information Processing Purposes |DATA TAGGING	Attach data tags containing the following purposes to [Assignment: organization-defined elements of personally identifiable information]: [Assignment: organization-defined processing purposes].	
PT-03(2)	Personally Identifiable Information Processing Purposes |AUTOMATION	Track processing purposes of personally identifiable information using [Assignment: organization-defined automated mechanisms].	
PT-04	Consent	Implement [Assignment: organization-defined tools or mechanisms] for individuals to consent to the processing of their personally identifiable information prior to its collection that facilitate individuals' informed decision-making.	
PT-04(1)	Consent | TAILORED CONSENT	Provide [Assignment: organization-defined mechanisms] to allow individuals to tailor processing permissions to selected elements of personally identifiable information.	

PT-04(2)	JUST-IN-TIME CONSENT	Present [Assignment: organization-defined consent mechanisms] to individuals at [Assignment: organization-defined frequency] and in conjunction with [Assignment: organization-defined personally identifiable information processing].	Are supply chain risks associated with organization-defined systems, system components, and system services assessed? Is the supply chain risk assessment updated at an organization-defined set 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?
PT-04(3)	REVOCATION	Implement [Assignment: organization-defined tools or mechanisms] for individuals to revoke consent to the processing of their personally identifiable information.	
PT-05	Privacy Notice	Provide notice to individuals about the processing of personally identifiable information that: a. Is available to individuals upon first interacting with an organization, and subsequently at [Assignment: organization-defined frequency]; b. Is clear and easy-to-understand, expressing information about personally identifiable information processing in plain language; c. Identifies the authority that authorizes the processing of personally identifiable information; d. Identifies the purposes for which personally identifiable information is to be processed; and e. Includes [Assignment: organization-defined information].	
PT-05(1)	JUST-IN-TIME NOTICE	Present notice of personally identifiable information processing to individuals at a time and location where the individual provides personally identifiable information or in conjunction with a data action, or [Assignment: organization-defined frequency].	

PT-05(2)	PRIVACY ACT STATEMENTS	Include Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.	Has a public reporting channel been established for receiving reports of vulnerabilities in organizational systems and system components?
PT-06	System of Records Notice	For systems that process information that will be maintained in a Privacy Act system of records: a. Draft system of records notices in accordance with OMB guidance and submit new and significantly modified system of records notices to the OMB and appropriate congressional committees for advance review; b. Publish system of records notices in the Federal Register; and c. Keep system of records notices accurate, up-to-date, and scoped in accordance with policy.	Are findings from security and privacy assessments, monitoring, and audits responded to in accordance with organizational risk tolerance?
PT-06(1)	ROUTINE USES	Review all routine uses published in the system of records notice at [Assignment: organization-defined frequency] to ensure continued accuracy, and to ensure that routine uses continue to be compatible with the purpose for which the information was collected.	Are privacy impact assessments (PIAs) conducted for systems, programs, or other activities before: (Select all that apply) a. Developing or procuring information technology that processes personally identifiable information (PII); and b. Initiating a new collection of PII that will be processed using information technology and includes PII permitting the physical or virtual (online) contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, ten or more individuals, other than agencies, instrumentalities, or employees of the federal government.

PT-06(2)	EXEMPTION RULES	Review all Privacy Act exemptions claimed for the system of records at [Assignment: organization-defined frequency] to ensure they remain appropriate and necessary in accordance with law, that they have been promulgated as regulations, and that they are accurately described in the system of records notice.	Are critical system components and functions identified by performing a criticality analysis for organization-defined systems, system components, or system services at organization-defined decision points in the system development life cycle?
PT-07	Specific Categories of Personally Identifiable Information	Apply [Assignment: organization-defined processing conditions] for specific categories of personally identifiable information.	
PT-07(1)	SOCIAL SECURITY NUMBERS	When a system processes Social Security numbers: (a) Eliminate unnecessary collection, maintenance, and use of Social Security numbers, and explore alternatives to their use as a personal identifier; (b) Do not deny any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his or her Social Security number; and (c) Inform any individual who is asked to disclose his or her Social Security number whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.	
PT-07(2)	FIRST AMENDMENT INFORMATION	Prohibit the processing of information describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual or unless pertinent to and within the scope of an authorized law enforcement activity.	

PT-08	Computer Matching Requirements	When a system or organization processes information for the purpose of conducting a matching program: a. Obtain approval from the Data Integrity Board to conduct the matching program; b. Develop and enter into a computer matching agreement; c. Publish a matching notice in the Federal Register; d. Independently verify the information produced by the matching program before taking adverse action against an individual, if required; and e. Provide individuals with notice and an opportunity to contest the findings before taking adverse action against an individual.	
RA-01	(Risk Assessment) 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	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	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.	

RA-03(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.	Are supply chain risks associated with organization-defined systems, system components, and system services assessed? Is the supply chain risk assessment updated at an organization-defined set 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	Vulnerability Monitoring and 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(11)	Vulnerability Monitoring and Scanning | Public Disclosure Program	Establish a public reporting channel for receiving reports of vulnerabilities in organizational systems and system components.	Has a public reporting channel been established for receiving reports of vulnerabilities in organizational systems and system components?
RA-05(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].	
RA-05(5)	Vulnerability Monitoring and Scanning | Privileged Access	Implement privileged access authorization to [Assignment: organization-defined system components] for [Assignment: organization-defined vulnerability scanning activities].	
RA-07	Risk Response	Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.	Are findings from security and privacy assessments, monitoring, and audits responded to in accordance with organizational risk tolerance?
RA-08	Privacy Impact Assessments	Conduct privacy impact assessments for systems, programs, or other activities before: a. Developing or procuring information technology that processes personally identifiable information; and b. Initiating a new collection of personally identifiable information that: 1. Will be processed using information technology; and 2. Includes personally identifiable information permitting the physical or virtual (online) contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, ten or more individuals, other than agencies, instrumentalities, or employees of the federal government.	Are privacy impact assessments (PIAs) conducted for systems, programs, or other activities before: (Select all that apply) a. Developing or procuring information technology that processes personally identifiable information (PII); and b. Initiating a new collection of PII that will be processed using information technology and includes PII permitting the physical or virtual (online) contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, ten or more individuals, other than agencies, instrumentalities, or employees of the federal government.

RA-09	Criticality Analysis	Identify critical system components and functions by performing a criticality analysis for [Assignment: organization-defined systems, system components, or system services] at [Assignment: organization-defined decision points in the system development life cycle].	Are critical system components and functions identified by performing a criticality analysis for organization-defined systems, system components, or system services at organization-defined decision points in the system development life cycle?
SA-01	(System and Services Acquisition) 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	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	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	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 i. Acceptance criteria.	
SA-04(1)	Acquisition Process | Functional Properties of Controls	Require the developer of the system, system component, or system service to provide a description of the functional properties of the controls to be implemented.	
SA-04(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-04(2)	Acquisition Process | Design and Implementation Information for Controls	Require the developer of the system, system component, or system service to provide design and implementation information for the controls that includes: [Selection (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; [Assignment: organization-defined design and implementation information]] at [Assignment: organization-defined level of detail].	

SA-04(9)	Acquisition Process | Functions, Ports, Protocols, and Services In Use	Require the developer of the system, system component, or system service to identify the functions, ports, protocols, and services intended for organizational use.	
SA-05	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	Security and Privacy Engineering 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-08(33)	Security and Privacy Engineering Principles | Minimization	Implement the privacy principle of minimization using [Assignment: organization-defined processes].	Has an organization-defined process been determined to implement the privacy principle of minimization? If yes, has this process been implemented?
SA-09	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-09(2)	External System Services | Identification of Functions, Ports, Protocols, and Services	Require providers of the following external system services to identify the functions, ports, protocols, and other services required for the use of such services: [Assignment: organization-defined external system services].	

SA-10	Developer Configuration Management	Require the developer of the system, system component, or system service to: a. Perform configuration management during system, component, or service [Selection (one or more): design; development; implementation; operation; disposal]; b. Document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items under configuration management]; c. Implement only organization-approved changes to the system, component, or service; d. Document approved changes to the system, component, or service and the potential security and privacy impacts of such changes; and e. Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel].	
SA-11	Developer Testing and Evaluation	Require the developer of the system, system component, or system service, at all post-design stages of the system development life cycle, to: a. Develop and implement a plan for ongoing security and privacy control assessments; b. Perform [Selection (one or more): unit; integration; system; regression] testing/evaluation [Assignment: organization-defined frequency] at [Assignment: organization-defined depth and coverage]; c. Produce evidence of the execution of the assessment plan and the results of the testing and evaluation; d. Implement a verifiable flaw remediation process; and e. Correct flaws identified during testing and evaluation.	

SA-15	Development Process, Standards, and Tools	a. Require the developer of the system, system component, or system service to follow a documented development process that: 1. Explicitly addresses security and privacy requirements; 2. Identifies the standards and tools used in the development process; 3. Documents the specific tool options and tool configurations used in the development process; and 4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and b. Review the development process, standards, tools, tool options, and tool configurations [Assignment: organization-defined frequency] to determine if the process, standards, tools, tool options and tool configurations selected and employed can satisfy the following security and privacy requirements: [Assignment: organization-defined security and privacy requirements].	
SA-15(3)	Development Process, Standards, and Tools | Criticality Analysis	Require the developer of the system, system component, or system service to perform a criticality analysis: (a) At the following decision points in the system development life cycle: [Assignment: organization-defined decision points in the system development life cycle]; and (b) At the following level of rigor: [Assignment: organization-defined breadth and depth of criticality analysis].	
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]].	

SC-01	(System and Communications 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] 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	Separation of System and User Functionality	Separate user functionality, including user interface services, from system management functionality.	
SC-04	Information In Shared System Resources	Prevent unauthorized and unintended information transfer via shared system resources.	

SC-05	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	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-07(24)	Boundary Protection | Personally Identifiable Information	For systems that process personally identifiable information: (a) Apply the following processing rules to data elements of personally identifiable information: [Assignment: organization-defined processing rules]; (b) Monitor for permitted processing at the external interfaces to the system and at key internal boundaries within the system; (c) Document each processing exception; and (d) Review and remove exceptions that are no longer supported.	
SC-07(3)	Boundary Protection | Access Points	Limit the number of external network connections to the system.	

SC-07(4)	Boundary Protection | External Telecommunications Services	(a) Implement a managed interface for each external telecommunication service; (b) Establish a traffic flow policy for each managed interface; (c) Protect the confidentiality and integrity of the information being transmitted across each interface; (d) Document each exception to the traffic flow policy with a supporting mission or business need and duration of that need; (e) Review exceptions to the traffic flow policy [Assignment: organization-defined frequency] and remove exceptions that are no longer supported by an explicit mission or business need; (f) Prevent unauthorized exchange of control plane traffic with external networks; (g) Publish information to enable remote networks to detect unauthorized control plane traffic from internal networks; and (h) Filter unauthorized control plane traffic from external networks.	
SC-07(5)	Boundary Protection | Deny By Default — Allow By Exception	Deny network communications traffic by default and allow network communications traffic by exception [Selection (one or more): at managed interfaces; for [Assignment: organization-defined systems]].	
SC-07(7)	Boundary Protection | Split Tunneling for Remote Devices	Prevent split tunneling for remote devices connecting to organizational systems unless the split tunnel is securely provisioned using [Assignment: organization-defined safeguards].	
SC-07(8)	Boundary Protection | Route Traffic to Authenticated Proxy Servers	Route [Assignment: organization-defined internal communications traffic] to [Assignment: organization-defined external networks] through authenticated proxy servers at managed interfaces.	
SC-08	Transmission Confidentiality and Integrity	Protect the [Selection (one or more): confidentiality; integrity] of transmitted information.	

SC-08(1)	Transmission Confidentiality and Integrity | Cryptographic Protection	Implement cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.	
SC-10	Network Disconnect	Terminate the network connection associated with a communications session at the end of the session or after [Assignment: organization-defined time period] of inactivity.	
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	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	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	Public Key Infrastructure Certificates	a. Issue public key certificates under an [Assignment: organization-defined certificate policy] or obtain public key certificates from an approved service provider; and b. Include only approved trust anchors in trust stores or certificate stores managed by the organization.	
SC-18	Mobile Code	a. Define acceptable and unacceptable mobile code and mobile code technologies; and b. Authorize, monitor, and control the use of mobile code within the system.	
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	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	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	Session Authenticity	Protect the authenticity of communications sessions.	
SC-28	Protection of Information At Rest	Protect the [Selection (one or more): confidentiality; integrity] of the following information at rest: [Assignment: organization-defined information at rest].	
SC-28(1)	Protection of Information At Rest | Cryptographic Protection	Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information].	
SC-39	Process Isolation	Maintain a separate execution domain for each executing system process.	

SI-01	(System and Information Integrity) 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	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-02(2)	Flaw Remediation | Automated Flaw Remediation Status	Determine if system components have applicable security-relevant software and firmware updates installed using [Assignment: organization-defined automated mechanisms] [Assignment: organization-defined frequency].	Is personally identifiable information (PII) being processed in the information life cycle limited? If yes, has the organization determined what elements the PII is limited to?
SI-03	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.	Has the organization determined techniques to use to minimize the use of personally identifiable information (PII) for research, testing, or training?

SI-04	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]].	Has the organization determined techniques to dispose of, destroy, or erase information following the retention period?
SI-04(2)	System Monitoring | Automated Tools and Mechanisms for Real-Time Analysis	Employ automated tools and mechanisms to support near real-time analysis of events.	
SI-04(4)	System Monitoring | Inbound and Outbound Communications Traffic	(a) Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic; (b) Monitor inbound and outbound communications traffic [Assignment: organization-defined frequency] for [Assignment: organization-defined unusual or unauthorized activities or conditions].	

SI-04(5)	System Monitoring | System-Generated Alerts	Alert [Assignment: organization-defined personnel or roles] when the following system-generated indications of compromise or potential compromise occur: [Assignment: organization-defined compromise indicators].	
SI-05	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-07	Software, Firmware, and Information Integrity	a. Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: [Assignment: organization-defined software, firmware, and information]; and b. Take the following actions when unauthorized changes to the software, firmware, and information are detected: [Assignment: organization-defined actions].	

SI-07(1)	Software, Firmware, and Information Integrity | Integrity Checks	Perform an integrity check of [Assignment: organization-defined software, firmware, and information] [Selection (one or more): at startup; at [Assignment: organization-defined transitional states or security-relevant events]; [Assignment: organization-defined frequency]].	
SI-07(7)	Software, Firmware, and Information Integrity | Integration of Detection and Response	Incorporate the detection of the following unauthorized changes into the organizational incident response capability: [Assignment: organization-defined security-relevant changes to the system].	
SI-08	Spam Protection	a. Employ spam protection mechanisms at system entry and exit points to detect and act on unsolicited messages; and b. Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.	
SI-08(2)	Spam Protection | Automatic Updates	Automatically update spam protection mechanisms [Assignment: organization-defined frequency].	
SI-10	Information Input Validation	Check the validity of the following information inputs: [Assignment: organization-defined information inputs to the system].	
SI-11	Error Handling	a. Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited; and b. Reveal error messages only to [Assignment: organization-defined personnel or roles].	

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-12(1)	Information Management and Retention | Limit Personally Identifiable Information Elements	Limit personally identifiable information being processed in the information life cycle to the following elements of personally identifiable information: [Assignment: organization-defined elements of personally identifiable information].	Is personally identifiable information (PII) being processed in the information life cycle limited? If yes, has the organization determined what elements the PII is limited to?
SI-12(2)	Information Management and Retention | Minimize Personally Identifiable Information In Testing, Training, and Research	Use the following techniques to minimize the use of personally identifiable information for research, testing, or training: [Assignment: organization-defined techniques].	Has the organization determined techniques to use to minimize the use of personally identifiable information (PII) for research, testing, or training?
SI-12(3)	Information Management and Retention | Information Disposal	Use the following techniques to dispose of, destroy, or erase information following the retention period: [Assignment: organization-defined techniques].	Has the organization determined techniques to dispose of, destroy, or erase information following the retention period?
SI-16	Memory Protection	Implement the following controls to protect the system memory from unauthorized code execution: [Assignment: organization-defined controls].	

SI-18	Personally Identifiable Information Quality Operations	a. Check the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle [Assignment: organization-defined frequency]; and b. Correct or delete inaccurate or outdated personally identifiable information. Discussion: Personally identifiable information quality operations include the steps	Is the accuracy, relevance, timeliness, and completeness of personally identifiable information (PII) checked across the information life cycle at an organization-defined set frequency? Is inaccurate or outdated PII corrected or deleted?
SI-18(4)	Personally Identifiable Information Quality Operations | Individual Requests	Correct or delete personally identifiable information upon request by individuals or their designated representatives.	Is PII corrected or deleted upon request by individuals or their designated representatives?
SI-19	De-Identification	a. Remove the following elements of personally identifiable information from datasets: [Assignment: organization-defined elements of personally identifiable information]; and b. Evaluate [Assignment: organization-defined frequency] for effectiveness of de-identification.	Has the organization determined elements of personally identifiable information (PII) to remove from datasets? If yes, are those elements removed? Are these datasets evaluated at an organization-defined set frequency for effectiveness of de-identification?

SR-01	(Supply Chain Risk Management) 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].	Is there a supply chain risk management policy? If yes, does it address the following? Select all that apply: (a) 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 Are there procedures in place to facilitate the implementation of the supply chain risk management policy and the associated supply chain risk management controls? Has an organization-defined official been designated to manage the development, documentation, and dissemination of the supply chain risk management policy and procedures? Are the policy and procedures reviewed and updated at an organization-defined set frequency and following pre-determined organization-defined events?
SR-02	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.	Has a plan been developed for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the organization-defined systems, system components or system services? Is the supply chain risk management plan reviewed and updated at an organization-defined set frequency to address threat, organizational or environmental changes? Is the supply chain risk management plan protected from unauthorized disclosure and modification?

SR-02(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].	Has a supply chain risk management team been established? If yes, have the personnel, roles, and responsibilities to lead and support the SCRM activities been determined? Have the supply chain risk management activities been determined?
SR-03	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]].	Has a process(es) been established to identify and address weaknesses or deficiencies in the supply chain elements and processes of organization-defined system or system component in coordination with organization-defined supply chain personnel? If yes, have the system or system component been determined? Have the supply chain personnel been determined? Have organization-defined supply chain controls been determined and employed 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? Have the selected and implemented supply chain processes and controls documented? If yes, where? a) security and privacy plans; b) supply chain risk management plan; c) organization-defined document.
SR-05	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].	Have organization-defined acquisition strategies, contract tools, and procurement methods been determined and employed to protect against, identify, and mitigate supply chain risks?

SR-06	Supplier Assessments and Reviews	Assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide [Assignment: organization-defined frequency].	Are the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide assessed and reviewed at an organization-defined set frequency?
SR-08	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]].	Have agreements and procedures been established with entities involved in the supply chain for the system, system component, or system service? If yes, select all that apply to the purpose of those agreements and procedures: a) notification of supply chain compromises; b) results of assessments or audits; c) organization-defined information.
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].	Have the system or system components been determined to be inspected to detect tampering? If yes, at what frequency are the system or system components inspected? a) at random; b) at an organization-defined set frequency, c) upon organization-defined indications of need for inspection.
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]].	Has an anti-counterfeit policy and procedure been developed and implemented that include the means to detect and prevent counterfeit components from entering the system? If yes, select all that apply as to who counterfeit system components are reported: a) source of counterfeit component; b) organization-defined external reporting organizations c) organization-defined personnel or roles.

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).	Have organization-defined personnel or roles been determined to train to detect counterfeit system components (including hardware, software, and firmware)? If yes, is the training conducted?
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].	Have organization-defined system components been determined to maintain configuration control over the system components awaiting service or repair and serviced or repaired components awaiting return to service? If yes, is the configuration control over those system components managed?
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].	Regarding disposal, have organization-defined data, documentation, tools, or system components been determined? If yes, have the organization-defined techniques and methods been determined for disposal of the above?