Georgia Enterprise PSGs Organized by NIST Control Families

Instructions: Click on the family you wish to review.

Access Control (AC)

NIST #	NIST Control Statement	Applicable State PSG
AC-1	Access Control Policy and Procedures. The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the access control policy and associated access controls; and b. Reviews and updates the current: 1. Access control policy [Assignment: organization-defined frequency]; and 2. Access control procedures [Assignment: organization-defined frequency].	PS-08-009 Access Control SM-15-001 Data Steward
AC-2	Account Management. The organization: a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: [Assignment: organization-defined information system account types]; b. Assigns account managers for information system accounts; c. Establishes conditions for group and role membership; d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account; e. Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts; f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions]; g. Monitors the use of, information system accounts; h. Notifies account managers: 1. When accounts are no longer required; 2. When users are terminated or transferred; and 3. When individual information system usage or need-to-know changes; i. Authorizes access to the information system based on: 1. A valid access authorization; 2. Intended system usage; and 3. Other attributes as required by the organization or associated missions/business functions; j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency]; and k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.	SS-08-010 Authorization and Access Management
AC-3	Access Enforcement. The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	PS-08-028 Public Access Systems SS-08-048 Network Access and Session Controls SS-08-049 Web and E-Commerce Security SM-15-001 Data Steward

AC-4	Information Flow Enforcement. The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].	PS-08-027 Network Security Controls PS-08-023 Remote Access SS-08-038 Secure Remote Access PS-08-030 Network Security - Information Flow SS-08-044 Outsourced IT Services and Third-Party Interconnections SM-15-001 Data Steward
AC-5	Separation of Duties. The organization: a. Separates [Assignment: organization-defined duties of individuals]; b. Documents separation of duties of individuals; and c. Defines information system access authorizations to support separation of duties.	SS-08-025 System Lifecycle Management
AC-6	Least Privilege. The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	SS-08-010 Authorization and Access Management
AC-7	Unsuccessful Logon Attempts. The information system: a. Enforces 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: locks the account/node for an [Assignment: organization-defined time period]; locks the account/node until released by an administrator; delays next logon prompt according to [Assignment: organization-defined delay algorithm]] when the maximum number of unsuccessful attempts is exceeded.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
AC-8	System Use Notification The information system: a. Displays to users [Assignment: organization-defined system use notification message or banner] before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that: 1. Users are accessing a U.S. Government information system; 2. Information system usage may be monitored, recorded, and subject to audit; 3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and 4. Use of the information system indicates consent to monitoring and recording; b. Retains 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 information system; and c. For publicly accessible systems: 1. Displays system use information [Assignment: organization-defined conditions], before granting further access; 2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and 3. Includes a description of the authorized uses of the system.	SS-08-001 Appropriate Use and Monitoring

AC-9	Previous Logon (Access) Notification. The information system notifies the user, upon successful logon (access) to the system, of the date and time of the last logon (access).	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
AC-10	Concurrent Session Control. The information system limits the number of concurrent sessions for each [Assignment: organization-defined account and/or account type] to [Assignment: organization-defined number].	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
AC-11	Session Lock. The information system: a. Prevents further access to the system by initiating a session lock after [Assignment: organization-defined time period] of inactivity or upon receiving a request from a user; and b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.	SS-08-048 Network Access and Session Controls
AC-12	Session Termination. The information system automatically terminates a user session after [Assignment: organization-defined conditions or trigger events requiring session disconnect].	SS-08-048 Network Access and Session Controls
AC-13	Supervision and Review — Access Control. [Withdrawn: Incorporated into AC-2 and AU-6].	Withdrawn: Incorporated into AC-2 and AU-6
AC-14	Permitted Actions without Identification or Authentication. The organization: a. Identifies [Assignment: organization-defined user actions] that can be performed on the information system without identification or authentication consistent with organizational missions/business functions; and b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.	SS-08-010 Authorization and Access Management
AC-15	Automated Marking. [Withdrawn: Incorporated into MP-3].	Withdrawn: Incorporated into MP-3
AC-16	Security Attributes. The organization: a. Provides the means to associate [Assignment: organization-defined types of security attributes] having [Assignment: organization-defined security attribute values] with information in storage, in process, and/or in transmission; b. Ensures that the security attribute associations are made and retained with the information; c. Establishes the permitted [Assignment: organization-defined security attributes] for [Assignment: organization-defined information systems]; and d. Determines the permitted [Assignment: organization-defined values or ranges] for each of the established security attributes.	PS-08-012 Data and Asset Categorization SS-08-014 Data Categorization - Impact Level SS-08-002 Classification of Personal Information SM-15-001 Data Steward SS-15-001 Data Storage Location
AC-17	Remote Access. The organization: a. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and b. Authorizes remote access to the information system prior to allowing	PS-08-023 Remote Access SS-08-038 Secure Remote Access SS-08-037 Teleworking and Remote Access GM-11-002 Social Media Guideline

	such connections.	
AC-18	Wireless Access. The organization: a. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and b. Authorizes wireless access to the information system prior to allowing such connections.	SS-08-039 Wireless and Mobile Computing
AC-19	Access Control for Mobile Devices. The organization: a. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and b. Authorizes the connection of mobile devices to organizational information systems.	SS-08-039 Wireless and Mobile Computing SS-12-002 Non-State Technology and Computing Devices
AC-20	Use of External Information Systems. The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to: a. Access the information system from external information systems; and b. Process, store, or transmit organization-controlled information using external information systems.	SS-12-002 Non-State Technology and Computing Devices SS-08-013 Third Party Security Requirements SA-14-003 Requirements to Use Cloud Services SO-10-003 – Enterprise Operational Environment
AC-21	Information Sharing. The organization: a. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for [Assignment: organization-defined information sharing circumstances where user discretion is required]; and b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions.	PM-07-003 Statewide Data Sharing SS-08-013 Third Party Security Requirements SM-15-001 Data Steward
AC-22	Publicly Accessible Content. The organization: a. Designates individuals authorized to post information onto a publicly accessible information system; b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information; c. Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and d. Reviews the content on the publicly accessible information system for nonpublic information [Assignment: organization-defined frequency] and removes such information, if discovered.	GM-11-002 Social Media Guideline SS-08-049 Web and E-Commerce Security
AC-23	Data Mining Protection. The organization employs [Assignment: organization-defined data mining prevention and detection techniques] for [Assignment: organization-defined data storage objects] to adequately detect and protect against data mining.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.

AC-24	Access Control Decisions. The organization establishes procedures to ensure [Assignment: organization-defined access control decisions] are applied to each access request prior to access enforcement.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
AC-25	Reference Monitor. The information system implements a reference monitor for [Assignment: organization- defined access control policies] that is tamperproof, always invoked, and small enough to be subject to analysis and testing, the completeness of which can be assured.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.

Return to: Instructions

Awareness & Training (AT)

NIST #	NIST Control Statement	Applicable State PSG
AT-1	Security Awareness and Training Policy and Procedures. The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and b. Reviews and updates the current: 1. Security awareness and training policy [Assignment: organization-defined frequency]; and 2. Security awareness and training procedures [Assignment: organization-defined frequency].	PS-08-010 Security Awareness Program
AT-2	Security Awareness Training. The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors): a. As part of initial training for new users; b. When required by information system changes; and c. [Assignment: organization-defined frequency] thereafter.	SS-08-012 Security Education and Awareness SS-08-017 Personnel Identity Verification and Screening
AT-3	Role-Based Security Training. The organization provides role-based security training to personnel with assigned security roles and responsibilities: a. Before authorizing access to the information system or performing assigned duties; b. When required by information system changes; and c. [Assignment: organization-defined frequency] thereafter.	SS-08-012 Security Education and Awareness SS-08-032 System Implementation and Acceptance
AT-4	Security Training Records. The organization: a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and b. Retains individual training records for [Assignment: organization-defined time period].	SS-08-012 Security Education and Awareness
AT-5	Contacts with Security Groups and Associations [Withdrawn: Incorporated into PM-15].	Withdrawn: Incorporated into PM-15

Return to: Instructions

Audit and Accountability (AU)

NIST #	NIST Control Statement	Applicable State PSG
AU-1	Audit and Accountability Policy and Procedures. The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and b. Reviews and updates the current: 1. Audit and accountability policy [Assignment: organization-defined frequency]; and 2. Audit and accountability procedures [Assignment: organization-defined frequency].	PS-08-022 Security Log Management
AU-2	Audit Events. The organization: a. Determines that the information system is capable of auditing the following events: [Assignment: organization-defined auditable events]; b. Coordinates the security audit function with other organizational entities requiring audit- related information to enhance mutual support and to help guide the selection of auditable events; c. Provides a rationale for why the auditable events are deemed to be adequate to support after- the-fact investigations of security incidents; and d. Determines that the following events are to be audited within the information system: [Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event].	SS-08-036 Log Management Infrastructure
AU-3	Content of Audit Records. The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.	SS-08-036 Log Management Infrastructure
AU-4	Audit Storage Capacity. The organization allocates audit record storage capacity in accordance with [Assignment: organization-defined audit record storage requirements].	SS-08-036 Log Management Infrastructure
AU-5	Response to Audit Processing Failures. The information system: a. Alerts [Assignment: organization-defined personnel or roles] in the event of an audit processing failure; and b. Takes the following additional actions: [Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)].	There are no PSGs published for this topic; however, the topic is under review for future PSGs.

AU-6	Audit Review, Analysis, and Reporting. The organization: a. Reviews and analyzes information system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity]; and b. Reports findings to [Assignment: organization-defined personnel or roles].	SS-08-036 Log Management Infrastructure
AU-7	Audit Reduction and Report Generation. The information system provides an audit reduction and report generation capability that: a. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and b. Does not alter the original content or time ordering of audit records.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
AU-8	Time Stamps. The information system: a. Uses internal system clocks to generate time stamps for audit records; and b. Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets [Assignment: organization-defined granularity of time measurement].	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
AU-9	Protection of Audit Information. The information system protects audit information and audit tools from unauthorized access, modification, and deletion.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
AU-10	Non-repudiation. The information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed [Assignment: organization-defined actions to be covered by non-repudiation].	PS-08-024 Use of Cryptography SS-08-040 Cryptographic Controls
AU-11	Audit Record Retention. The organization retains audit records for [Assignment: organization-defined time period consistent with records retention policy] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
AU-12	Audit Generation. The information system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at [Assignment: organization-defined information system components]; b. Allows [Assignment: organization-defined personnel or roles] to select which auditable events are to be audited by specific components of the information system; and c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
AU-13	Monitoring for Information Disclosure. The organization monitors [Assignment: organization-defined open source information and/or information sites] [Assignment: organization-defined frequency] for evidence of unauthorized disclosure of organizational information.	SM-15-001 Data Steward
AU-14	Session Audit. The information system provides the capability for authorized users to select a user session to capture/record or view/hear.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
AU-15	Alternate Audit Capability. The organization provides an alternate audit capability in the event of a failure in primary audit capability that provides [Assignment: organization-defined alternate audit functionality].	There are no PSGs published for this topic; however, the topic is under review for future PSGs.

AU-16	Cross-Organizational Auditing. The organization employs [Assignment: organization-defined methods] for coordinating [Assignment: organization-defined audit information] among external organizations when audit information is transmitted across organizational boundaries.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.

Return to: Instructions

Security Assessment and Authorization (CA)

NIST #	NIST Control Statement	Applicable State PSG
CA-1	Security Assessment and Authorization Policies and Procedures. The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and b. Reviews and updates the current: 1. Security assessment and authorization policy [Assignment: organization-defined frequency]; and 2. Security assessment and authorization procedures [Assignment: organization-defined frequency].	PS-08-029 Security Controls Review and Assessments SS-08-042 Independent Security Assessments SM-06-001 Independent Verification and Validation
CA-2	Security Assessments. The organization: a. Develops a security assessment plan that describes the scope of the assessment including: 1. Security controls and control enhancements under assessment; 2. Assessment procedures to be used to determine security control effectiveness; and 3. Assessment environment, assessment team, and assessment roles and responsibilities; b. Assesses the security controls in the information 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 requirements; c. Produces a security assessment report that documents the results of the assessment; and d. Provides the results of the security control assessment to [Assignment: organization-defined individuals or roles].	SS-08-042 Independent Security Assessments
CA-3	System Interconnections. The organization: a. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements; b. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and c. Reviews and updates Interconnection Security Agreements [Assignment: organization-defined frequency].	SS-08-028 System Security Plans PM-07-003 Statewide Data Sharing SM-15-001 Data Steward
CA-4	Security Certification. [Withdrawn: Incorporated into CA-2].	Withdrawn: Incorporated into CA-2

CA-5	Plan of Action and Milestones. The organization: a. Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and b. Updates existing plan of action and milestones [Assignment: organization-defined frequency] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.	SS-08-028 System Security Plans
CA-6	Security Authorization. The organization: a. Assigns a senior-level executive or manager as the authorizing official for the information system; b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and c. Updates the security authorization [Assignment: organization-defined frequency].	SS-08-032 System Implementation and Acceptance SA-10-009 – Deployment Certification
CA-7	Continuous Monitoring. The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored; b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring; c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; d. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy; e. Correlation and analysis of security-related information generated by assessments and monitoring; f. Response actions to address results of the analysis of security-related information; and g. Reporting the security status of organization and the information system to [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency].	SS-08-041 Risk Management Framework
CA-8	Penetration Testing. The organization conducts penetration testing [Assignment: organization-defined frequency] on [Assignment: organization-defined information systems or system components].	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
CA-9	Internal System Connections. The organization: a. Authorizes internal connections of [Assignment: organization-defined information system components or classes of components] to the information system; and b. Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.

Return to: Instructions

Configuration Management (CM)

NIST #	NIST Control Statement	Applicable State PSG
CM-1	Configuration Management Policy and Procedures. The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and b. Reviews and updates the current: 1. Configuration management policy [Assignment: organization-defined frequency]; and 2. Configuration management procedures [Assignment: organization-defined frequency].	PM-03-003 Enterprise Architecture PM-07-003 Statewide Data Sharing PM-13-002 Enterprise Application PS-08-015 Change Management SS-08-026 Operational Change Control
CM-2	Baseline Configuration. The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.	PM-13-002 Enterprise Application SM-13-003 Enterprise Application Creation and Management
CM-3	Configuration Change Control. The organization: a. Determines the types of changes to the information system that are configuration-controlled; b. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses; c. Documents configuration change decisions associated with the information system; d. Implements approved configuration-controlled changes to the information system; e. Retains records of configuration-controlled changes to the information system for [Assignment: organization-defined time period]; f. Audits and reviews activities associated with configuration-controlled changes to the information system; and g. Coordinates and provides oversight for configuration change control activities through [Assignment: organization-defined configuration change control element (e.g., committee, board] that convenes [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined configuration change conditions]].	PS-08-015 Change Management SS-08-026 Operational Change Control
CM-4	Security Impact Analysis. The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.	SS-08-026 Operational Change Control
CM-5	Access Restrictions for Change. The organization defines documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.

CM-6	Configuration Settings. The organization: a. Establishes and documents configuration settings for information technology products employed within the information system using [Assignment: organization-defined security configuration checklists] that reflect the most restrictive mode consistent with operational requirements; b. Implements the configuration settings; c. Identifies, documents, and approves any deviations from established configuration settings for [Assignment: organization-defined information system components] based on [Assignment: organization-defined operational requirements]; and d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
CM-7	Least Functionality. The organization: a. Configures the information system to provide only essential capabilities; and b. Prohibits or restricts the use of the following functions, ports, protocols, and/or services: [Assignment: organization-defined prohibited or restricted functions, ports, protocols, and/or services].	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
CM-8	Information System Component Inventory. The organization: a. Develops and documents an inventory of information system components that: 1. Accurately reflects the current information system; 2. Includes all components within the authorization boundary of the information system; 3. Is at the level of granularity deemed necessary for tracking and reporting; and 4. Includes [Assignment: organization-defined information deemed necessary to achieve effective information system component accountability]; and b. Reviews and updates the information system component inventory [Assignment: organization-defined frequency].	PS-08-002 Accountability of Assets PS-08-012 Data and Asset Categorization SS-08-014 Data Categorization - Impact Level SS-08-053 Information Technology Reporting SS-15-001 Data Storage Location
CM-9	Configuration Management Plan. The organization develops, documents, and implements a configuration management plan for the information 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 information system and places the configuration items under configuration management; and d. Protects the configuration management plan from unauthorized disclosure and modification.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.

CM-10	Software Usage Restrictions. The organization: a. Uses software and associated documentation in accordance with contract agreements and copyright laws; b. Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and c. Controls and documents 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.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
CM-11	User-Installed Software. The organization: a. Establishes [Assignment: organization-defined policies] governing the installation of software by users; b. Enforces software installation policies through [Assignment: organization-defined methods]; and c. Monitors policy compliance at [Assignment: organization-defined frequency].	There are no PSGs published for this topic; however, the topic is under review for future PSGs.

Return to: Instructions

Contingency Planning (CP)

NIST #	NIST Control Statement	Applicable State PSG
CP-1	Contingency Planning Policy and Procedures. The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls; and b. Reviews and updates the current: 1. Contingency planning policy [Assignment: organization-defined frequency]; and 2. Contingency planning procedures [Assignment: organization-defined frequency].	PS-08-025 Business Continuity and Disaster Recovery SS-08-045 Contingency Planning
CP-2	Contingency Plan. The organization: a. Develops a contingency plan for the information system that: 1. Identifies essential missions 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 missions and business functions despite an information system disruption, compromise, or failure; 5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and 6. Is reviewed and approved by [Assignment: organization-defined personnel or roles]; b. Distributes copies of the contingency plan to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; c. Coordinates contingency planning activities with incident handling activities; d. Reviews the contingency plan for the information system [Assignment: organization-defined frequency]; e. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; f. Communicates contingency plan changes to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; and g. Protects the contingency plan from unauthorized disclosure and modification.	PS-08-025 Business Continuity and Disaster Recovery SS-08-045 Contingency Planning

CP-3	Contingency Training. The organization provides contingency training to information system users consistent with assigned roles and responsibilities: a. Within [Assignment: organization-defined time period] of assuming a contingency role or responsibility; b. When required by information system changes; and c. [Assignment: organization-defined frequency] thereafter.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
CP-4	Contingency Plan Testing. The organization: a. Tests the contingency plan for the information system [Assignment: organization-defined frequency] using [Assignment: organization-defined tests] to determine the effectiveness of the plan and the organizational readiness to execute the plan; b. Reviews the contingency plan test results; and c. Initiates corrective actions, if needed.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
CP-5	Contingency Plan Update. [Withdrawn: Incorporated into CP-2].	Withdrawn: Incorporated into CP-2
CP-6	Alternate Storage Site. The organization: a. Establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information; and b. Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.	PS-08-026 Media Controls GM-13-001 Retention of Data Backup Media and Records Management Media
CP-7	Alternate Processing Site. The organization: a. Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of [Assignment: organization-defined information system operations] for essential missions/business functions within [Assignment: organization-defined time period consistent with recovery time and recovery point objectives] when the primary processing capabilities are unavailable; b. Ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and c. Ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site.	SS-08-045 Contingency Planning
CP-8	Telecommunications Services. The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of [Assignment: organization-defined information system operations] for essential missions 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.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.

CP-9	Information System Backup. The organization: a. Conducts backups of user-level information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; b. Conducts backups of system-level information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; c. Conducts backups of information system documentation including security-related documentation [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; and d. Protects the confidentiality, integrity, and availability of backup information at storage locations.	PS-08-026 Media Controls GM-13-001 Retention of Data Backup Media and Records Management Media
CP-10	Information System Recovery and Reconstitution. The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.	SS-08-046 Disaster Recovery - System Backup
CP-11	Alternate Communications Protocols. The information system provides the capability to employ [Assignment: organization- defined alternative communications protocols] in support of maintaining continuity of operations.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
CP-12	Safe Mode. The information system, when [Assignment: organization-defined conditions] are detected, enters a safe mode of operation with [Assignment: organization-defined restrictions of safe mode of operation].	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
CP-13	Alternative Security Mechanisms. The organization employs [Assignment: organization-defined alternative or supplemental security mechanisms] for satisfying [Assignment: organization-defined security functions] when the primary means of implementing the security function is unavailable or compromised.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.

Return to: Instructions

Identification and Authentication (IA)

NIST #	NIST Control Statement	Applicable State PSG
IA-1	Identification and Authentication Policy and Procedures. The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and b. Reviews and updates the current: 1. Identification and authentication policy [Assignment: organization-defined frequency]; and 2. Identification and authentication procedures [Assignment: organization-defined frequency].	PS-08-006 Password Authentication SS-08-007 Password Security SS-08-008 Strong Password Use SS-08-010 Authorization and Access Management
IA-2	Identification and Authentication (Organizational Users). The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).	PS-08-028 Public Access Systems PS-08-006 Password Authentication SS-08-007 Password Security SS-08-008 Strong Password Use SS-08-011 Email Use and Protection
IA-3	Device Identification and Authentication. The information system uniquely identifies and authenticates [Assignment: organization- defined specific and/or types of devices] before establishing a [Selection (one or more): local; remote; network] connection.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
IA-4	Identifier Management. The organization manages information system identifiers by: a. Receiving authorization from [Assignment: organization-defined personnel or roles] to assign an individual, group, role, or device identifier; b. Selecting an identifier that identifies an individual, group, role, or device; c. Assigning the identifier to the intended individual, group, role, or device; d. Preventing reuse of identifiers for [Assignment: organization-defined time period]; and e. Disabling the identifier after [Assignment: organization-defined time period of inactivity].	PS-08-006 Password Authentication SS-08-007 Password Security SS-08-008 Strong Password Use SS-08-011 Email Use and Protection SS-08-010 Authorization and Access Management

IA-5	Authenticator Management. The organization manages information system authenticators by: 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; d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators; e. Changing default content of authenticators prior to information system installation; f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators; g. Changing/refreshing authenticators [Assignment: organization-defined time period by authenticator type]; h. Protecting authenticator content from unauthorized disclosure and modification; i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and j. Changing authenticators for group/role accounts when membership to those accounts changes.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
IA-6	Authenticator Feedback. The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
IA-7	Cryptographic Module Authentication. The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
IA-8	Identification and Authentication (Non-Organizational Users). The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).	PS-08-011 Third-Party Access SS-08-013 Third-Party Security Requirements
IA-9	Service Identification and Authentication. The organization identifies and authenticates [Assignment: organization-defined information system services] using [Assignment: organization-defined security safeguards].	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
IA-10	Adaptive Identification and Authentication. The organization requires that individuals accessing the information system employ [Assignment: organization-defined supplemental authentication techniques or mechanisms] under specific [Assignment: organization-defined circumstances or situations].	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
IA-11	Re-authentication. The organization requires users and devices to re-authenticate when [Assignment: organization-defined circumstances or situations requiring re-authentication].	There are no PSGs published for this topic; however, the topic is under review for future PSGs.

Return to: Instructions

Incident Response (IR)

NIST #	NIST Control Statement	Applicable State PSG
IR-1	Incident Response Policy and Procedures. The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and b. Reviews and updates the current: 1. Incident response policy [Assignment: organization-defined frequency]; and 2. Incident response procedures [Assignment: organization-defined frequency].	PS-08-004 Computer Security Incident Management SS-08-004 Incident Response and Reporting
IR-2	Incident Response Training. The organization provides incident response training to information system users consistent with assigned roles and responsibilities: a. Within [Assignment: organization-defined time period] of assuming an incident response role or responsibility; b. When required by information system changes; and c. [Assignment: organization-defined frequency] thereafter.	SS-08-012 Security Education and Awareness
IR-3	Incident Response Testing. The organization tests the incident response capability for the information system [Assignment: organization-defined frequency] using [Assignment: organization-defined tests] to determine the incident response effectiveness and documents the results.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
IR-4	Incident Handling. The organization: a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; b. Coordinates incident handling activities with contingency planning activities; and c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.	SM-15-001 Data Steward
IR-5	Incident Monitoring. The organization tracks and documents information system security incidents.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
IR-6	Incident Reporting. The organization: a. Requires personnel to report suspected security incidents to the organizational incident response capability within [Assignment: organization-defined time period]; and b. Reports security incident information to [Assignment: organization-defined authorities].	PS-08-004 Computer Security Incident Management SS-08-004 Incident Response and Reporting SM-15-001 Data Steward
IR-7	Incident Response Assistance. The organization provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.

IR-8	Incident Response Plan. The organization: a. Develops 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; and 8. Is reviewed and approved by [Assignment: organization-defined personnel or roles]; b. Distributes copies of the incident response plan to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; c. Reviews the incident response plan [Assignment: organization-defined frequency]; d. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; e. Communicates incident response plan changes to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; and f. Protects the incident response plan from unauthorized disclosure and modification.	SM-15-001 Data Steward
IR-9	Information Spillage Response. The organization responds to information spills by: a. Identifying the specific information involved in the information system contamination; b. Alerting [Assignment: organization-defined personnel or roles] of the information spill using a method of communication not associated with the spill; c. Isolating the contaminated information system or system component; d. Eradicating the information from the contaminated information system or component; e. Identifying other information systems or system components that may have been subsequently contaminated; and f. Performing other [Assignment: organization-defined actions].	SM-15-001 Data Steward
IR-10	Integrated Information Security Analysis Team. The organization establishes an integrated team of forensic/malicious code analysts, tool developers, and real-time operations personnel.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.

Return to: Instructions

Maintenance (MA)

NIST#	NIST Control Statement	Applicable State PSG
MA-1	System Maintenance Policy and Procedures. The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; and b. Reviews and updates the current: 1. System maintenance policy [Assignment: organization-defined frequency]; and 2. System maintenance procedures [Assignment: organization-defined frequency].	PS-08-018 Systems and Development Lifecycle SS-08-025 System Lifecycle Management SM-10-006 Performance Lifecycle Framework
MA-2	Controlled Maintenance. The organization: a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements; b. Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location; c. Requires that [Assignment: organization-defined personnel or roles] explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs; d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and f. Includes [Assignment: organization-defined maintenance-related information] in organizational maintenance records.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
MA-3	Maintenance Tools. The organization approves, controls, and monitors information system maintenance tools.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
MA-4	Nonlocal Maintenance. The organization: a. Approves and monitors nonlocal maintenance and diagnostic activities; b. Allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system; c. Employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions; d. Maintains records for nonlocal maintenance and diagnostic activities; and e. Terminates session and network connections when nonlocal maintenance is completed.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.

MA-5	Maintenance Personnel. The organization: a. Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel; b. Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and c. Designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
MA-6	Timely Maintenance. The organization obtains maintenance support and/or spare parts for [Assignment: organization-defined information system components] within [Assignment: organization-defined time period] of failure.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.

Return to: Instructions

Media Protection (MP)

NIST #	NIST Control Statement	Applicable State PSG
MP-1	Media Protection Policy and Procedures. The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls; and b. Reviews and updates the current: 1. Media protection policy [Assignment: organization-defined frequency]; and 2. Media protection procedures [Assignment: organization-defined frequency].	PS-08-026 Media Controls SS-08-043 Media Protection and Handling GM-13-001 Retention of Data Backup Media and Records Management Media
MP-2	Media Access. The organization restricts access to [Assignment: organization-defined types of digital and/or non-digital media] to [Assignment: organization-defined personnel or roles].	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
MP-3	Media Marking. The organization: a. Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and b. Exempts [Assignment: organization-defined types of information system media] from marking as long as the media remain within [Assignment: organization-defined controlled areas].	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
MP-4	Media Storage. The organization: a. Physically controls and securely stores [Assignment: organization-defined types of digital and/or non-digital media] within [Assignment: organization-defined controlled areas]; and b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
MP-5	Media Transport. The organization: a. Protects and controls [Assignment: organization-defined types of information system media] during transport outside of controlled areas using [Assignment: organization-defined security safeguards]; b. Maintains accountability for information system media during transport outside of controlled areas; c. Documents activities associated with the transport of information system media; and d. Restricts the activities associated with the transport of information system media to authorized personnel.	SS-08-034 Surplus Electronic Media Disposal SS-08-035 Media Sanitization - Vendor Return

MP-6	Media Sanitization. The organization: a. Sanitizes [Assignment: organization-defined information system media] prior to disposal, release out of organizational control, or release for reuse using [Assignment: organization- defined sanitization techniques and procedures] in accordance with applicable federal and organizational standards and policies; and b. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.	SS-08-034 Surplus Electronic Media Disposal SS-08-035 Media Sanitization - Vendor Return
MP-7	Media Use. The organization [Selection: restricts; prohibits] the use of [Assignment: organization- defined types of information system media] on [Assignment: organization-defined information systems or system components] using [Assignment: organization-defined security safeguards].	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
MP-8	Media Downgrading. The organization: a. Establishes [Assignment: organization-defined information system media downgrading process] that includes employing downgrading mechanisms with [Assignment: organization- defined strength and integrity]; b. Ensures that the information system media downgrading process is commensurate with the security category and/or classification level of the information to be removed and the access authorizations of the potential recipients of the downgraded information; c. Identifies [Assignment: organization-defined information system media requiring downgrading]; and d. Downgrades the identified information system media using the established process.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.

Return to: Instructions

Physical and Environmental Protection (PE)

NIST #	NIST Control Statement	Applicable State PSG
PE-1	Physical and Environmental Protection Policy and Procedures. The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and b. Reviews and updates the current: 1. Physical and environmental protection policy [Assignment: organization-defined frequency]; and 2. Physical and environmental protection procedures [Assignment: organization-defined frequency].	PS-08-013 Physical and Environmental Security SS-08-015 Facilities Security SS-08-016 Computer Operations Center Security
PE-2	Physical Access Authorizations. The organization: a. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides; b. Issues authorization credentials for facility access; c. Reviews the access list detailing authorized facility access by individuals [Assignment: organization-defined frequency]; and d. Removes individuals from the facility access list when access is no longer required.	PS-08-011 Third-Party Access SS-08-015 Facilities Security SS-08-016 Computer Operations Center Security
PE-3	Physical Access Control. The organization: a. Enforces physical access authorizations at [Assignment: organization-defined entry/exit points to the facility where the information system resides] by; 1. Verifying individual access authorizations before granting access to the facility; and 2. Controlling ingress/egress to the facility using [Selection (one or more): [Assignment: organization-defined physical access control systems/devices]; guards]; b. Maintains physical access audit logs for [Assignment: organization-defined entry/exit points]; c. Provides [Assignment: organization-defined security safeguards] to control access to areas within the facility officially designated as publicly accessible; d. Escorts visitors and monitors visitor activity [Assignment: organization-defined circumstances requiring visitor escorts and monitoring]; e. Secures keys, combinations, and other physical access devices; f. Inventories [Assignment: organization-defined physical access devices] every [Assignment: organization-defined frequency]; and g. Changes combinations and keys [Assignment: organization-defined frequency] and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.	PS-08-013 Physical and Environmental Security PS-08-019 Outsourced Facilities Management SS-08-015 Facilities Security SS-08-016 Computer Operations Center Security SS-15-001 Data Storage Location

PE-4	Access Control for Transmission Medium. The organization controls physical access to [Assignment: organization-defined information system distribution and transmission lines] within organizational facilities using [Assignment: organization-defined security safeguards].	PS-08-013 Physical and Environmental Security PS-08-019 Outsourced Facilities Management SS-08-015 Facilities Security SS-08-016 Computer Operations Center Security
PE-5	Access Control for Output Devices. The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.	PS-08-013 Physical and Environmental Security PS-08-019 Outsourced Facilities Management SS-08-015 Facilities Security SS-08-016 Computer Operations Center Security
PE-6	Monitoring Physical Access. The organization: a. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents; b. Reviews physical access logs [Assignment: organization-defined frequency] and upon occurrence of [Assignment: organization-defined events or potential indications of events]; and c. Coordinates results of reviews and investigations with the organizational incident response capability.	PS-08-011 Third-Party Access SS-08-015 Facilities Security SS-08-016 Computer Operations Center Security
PE-7	Visitor Control. [Withdrawn: Incorporated into PE-2 and PE-3].	Withdrawn: Incorporated into PE-2 and PE-3
PE-8	Visitor Access Records. The organization: a. Maintains visitor access records to the facility where the information system resides for [Assignment: organization-defined time period]; and b. Reviews visitor access records [Assignment: organization-defined frequency].	PS-08-011 Third-Party Access SS-08-015 Facilities Security SS-08-016 Computer Operations Center Security
PE-9	Power Equipment and Cabling. The organization protects power equipment and power cabling for the information system from damage and destruction.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
PE-10	Emergency Shutoff. The organization: a. Provides the capability of shutting off power to the information system or individual system components in emergency situations; b. Places emergency shutoff switches or devices in [Assignment: organization-defined location by information system or system component] to facilitate safe and easy access for personnel; and c. Protects emergency power shutoff capability from unauthorized activation.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
PE-11	Emergency Power. The organization provides a short-term uninterruptible power supply to facilitate [Selection (one or more): an orderly shutdown of the information system; transition of the information system to long-term alternate power] in the event of a primary power source loss.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.

PE-12	Emergency Lighting. The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
PE-13	Fire Protection. The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
PE-14	Temperature and Humidity Controls. The organization: a. Maintains temperature and humidity levels within the facility where the information system resides at [Assignment: organization-defined acceptable levels]; and b. Monitors temperature and humidity levels [Assignment: organization-defined frequency].	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
PE-15	Water Damage Protection. The organization protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
PE-16	Delivery and Removal. The organization authorizes, monitors, and controls [Assignment: organization-defined types of information system components] entering and exiting the facility and maintains records of those items.	PS-08-013 Physical and Environmental Security PS-08-019 Outsourced Facilities Management SS-08-015 Facilities Security SS-08-016 Computer Operations Center Security SS-15-001 Data Storage Location
PE-17	Alternate Work Site The organization: a. Employs [Assignment: organization-defined security controls] at alternate work sites; b. Assesses as feasible, the effectiveness of security controls at alternate work sites; and c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
PE-18	Location of Information System Components. The organization positions information system components within the facility to minimize potential damage from [Assignment: organization-defined physical and environmental hazards] and to minimize the opportunity for unauthorized access.	SS-08-015 Facilities Security SS-08-016 Computer Operations Center Security
PE-19	Information Leakage. The organization protects the information system from information leakage due to electromagnetic signals emanations.	PS-08-013 Physical and Environmental Security PS-08-019 Outsourced Facilities Management SS-08-015 Facilities Security SS-08-016 Computer Operations Center Security
PE-20	Asset Monitoring and Tracking. The organization: a. Employs [Assignment: organization-defined asset location technologies] to track and monitor the location and movement of [Assignment: organization-defined assets] within [Assignment: organization-defined controlled areas]; and b. Ensures that asset location technologies are employed in accordance with applicable federal laws, Executive Orders, directives, regulations,	PS-08-002 Accountability of Assets

	policies, standards, and guidance.	

Return to: Instructions

Planning (PL)

NIST #	NIST Control Statement	Applicable State PSG
PL-1	Security Planning Policy and Procedures. The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security planning policy and associated security planning controls; and b. Reviews and updates the current: 1. Security planning policy [Assignment: organization-defined frequency]; and 2. Security planning procedures [Assignment: organization-defined frequency].	PS-08-005 Enterprise Information Security Charter SS-08-006 Information Security Management Organization SS-08-005 Information Security Infrastructure SM-15-001 Data Steward

PL-2	System Security Plan. The organization: a. Develops a security plan for the information system that: 1. Is consistent with the organization’s enterprise architecture; 2. Explicitly defines the authorization boundary for the system; 3. Describes the operational context of the information system in terms of missions and business processes; 4. Provides the security categorization of the information system including supporting rationale; 5. Describes the operational environment for the information system and relationships with or connections to other information systems; 6. Provides an overview of the security requirements for the system; 7. Identifies any relevant overlays, if applicable; 8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and 9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation; b. Distributes copies of the security plan and communicates subsequent changes to the plan to [Assignment: organization-defined personnel or roles]; c. Reviews the security plan for the information system [Assignment: organization-defined frequency]; d. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and e. Protects the security plan from unauthorized disclosure and modification.	SS-08-028 System Security Plans PS-08-018 Systems and Development Lifecycle SM-15-001 Data Steward
PL-3	System Security Plan Update. [Withdrawn: Incorporated into PL-2].	Withdrawn: Incorporated into PL-2
PL-4	Rules of Behavior. The organization: a. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; b. Receives a signed 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 information system; c. Reviews and updates the rules of behavior [Assignment: organization-defined frequency]; and d. Requires individuals who have signed a previous version of the rules of behavior to read and re-sign when the rules of behavior are revised/updated.	PS-08-003 – Appropriate Use of Information Technology Resources PS-08-012 Data and Asset Categorization PS-08-029 Security Controls Review and Assessments SS-08-002 Classification of Personal Information SS-08-009 – Electronic Communications Accountability SS-08-014 Data Categorization - Impact Level SS-08-001 Appropriate Use and Monitoring SS-08-003 Data Security-Electronic Records SM-15-001 Data Steward SS-15-001 Data Storage Location
PL-5	Privacy Impact Assessment. [Withdrawn: Incorporated into Appendix J, AR-2].	Withdrawn: Incorporated into Appendix J, AR-2
PL-6	Security-Related Activity Planning. [Withdrawn: Incorporated into PL-2].	Withdrawn: Incorporated into PL-2

PL-7	Security Concept of Operations. The organization: a. Develops a security Concept of Operations (CONOPS) for the information system containing at a minimum, how the organization intends to operate the system from the perspective of information security; and b. Reviews and updates the CONOPS [Assignment: organization-defined frequency].	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
PL-8	Information Security Architecture. The organization: a. Develops an information security architecture for the information system that: 1. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information; 2. Describes how the information security architecture is integrated into and supports the enterprise architecture; and 3. Describes any information security assumptions about, and dependencies on, external services; b. Reviews and updates the information security architecture [Assignment: organization-defined frequency] to reflect updates in the enterprise architecture; and c. Ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
PL-9	Central Management. The organization centrally manages [Assignment: organization-defined security controls and related processes].	There are no PSGs published for this topic; however, the topic is under review for future PSGs.

Return to: Instructions

Program Management (PM)

NIST #	NIST Control Statement	Applicable State PSG
PM-1	Information Security Program Plan. The organization: a. Develops and disseminates an organization-wide information security program plan that: 1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements; 2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 3. Reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical); and 4. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; b. Reviews the organization-wide information security program plan [Assignment: organization-defined frequency]; c. Updates the plan to address organizational changes and problems identified during plan implementation or security control assessments; and d. Protects the information security program plan from unauthorized disclosure and modification.	PS-08-005 Enterprise Information Security Charter
PM-2	Senior Information Security Officer. The organization appoints a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.	SS-08-006 Information Security Management Organization
PM-3	Information Security Resources. The organization: a. Ensures that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement; b. Employs a business case/Exhibit 300/Exhibit 53 to record the resources required; and c. Ensures that information security resources are available for expenditure as planned.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
PM-4	Plan of Action and Milestones Process. The organization: a. Implements a process for ensuring that plans of action and milestones for the security program and associated organizational information systems: 1. Are developed and maintained; 2. Document the remedial information security actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and 3. Are reported in accordance with OMB FISMA reporting requirements. b. Reviews plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.	PS-08-031 Information Security - Risk Management SS-08-041 Risk Management Framework

PM-5	Information System Inventory. The organization develops and maintains an inventory of its information systems.	PS-08-002 Accountability of Assets PS-08-012 Data and Asset Categorization
PM-6	Information Security Measures of Performance. The organization develops, monitors, and reports on the results of information security measures of performance.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
PM-7	Enterprise Architecture. The organization develops an enterprise architecture with consideration or information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.	PM-03-003 Enterprise Architecture
PM-8	Critical Infrastructure Plan. The organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
PM-9	Risk Management Strategy. The Organization: a. Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems; b. Implements the risk management strategy consistently across the organization; and c. Reviews and updates the risk management strategy [Assignment: organization-defined frequency] or as required, to address organizational changes.	PS-08-031 Information Security - Risk Management SS-08-005 Information Security Infrastructure SS-08-041 Risk Management Framework
PM-10	Security Authorization Process. The Organization: a. Manages (i.e., documents, tracks, and reports) the security state of organizational information systems and the environments in which those systems operate through security authorization processes; b. Designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and c. Fully integrates the security authorization processes into an organization-wide risk management program.	SS-08-027 System Operations Documentation
PM-11	Mission/Business Process Definition. The Organization: a. Defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and b. Determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until achievable protection needs are obtained.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
PM-12	Insider Threat Program. The organization implements an insider threat program that includes a cross-discipline insider threat incident handling team.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
PM-13	Information Security Workforce. The organization establishes an information security workforce development and improvement program.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.

PM-14	Testing, Training, and Monitoring. The Organization: a. Implements a process for ensuring that organizational plans for conducting security testing, training, and monitoring activities associated with organizational information systems: 1. Are developed and maintained; and 2. Continue to be executed in a timely manner; b. Reviews testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
PM-15	Contacts with Security Groups and Associations. The organization establishes and institutionalizes contact with selected groups and associations within the security community: a. To facilitate ongoing security education and training for organizational personnel; b. To maintain currency with recommended security practices, techniques, and technologies; and c. To share current security-related information including threats, vulnerabilities, and incidents.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
PM-16	Threat Awareness Program. The organization implements a threat awareness program that includes a cross-organization information-sharing capability.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.

Return to: Instructions

Personnel Security (PS)

NIST #	NIST Control Statement	Applicable State PSG
PS-1	Personnel Security Policy and Procedures. The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls; and b. Reviews and updates the current: 1. Personnel security policy [Assignment: organization-defined frequency]; and 2. Personnel security procedures [Assignment: organization-defined frequency].	PS-08-014 Personnel Security
PS-2	Position Risk Designation. The organization: a. Assigns a risk designation to all organizational positions; b. Establishes screening criteria for individuals filling those positions; and c. Reviews and updates position risk designations [Assignment: organization-defined frequency].	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
PS-3	Personnel Screening. The organization: a. Screens individuals prior to authorizing access to the information system; and b. Rescreens individuals according to [Assignment: organization-defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of such rescreening].	PS-08-014 Personnel Security SS-08-017 Personnel Identity Verification and Screening SS-08-013 Third-Party Security Requirements SS-08-044 Outsourced IT Services and Third-Party Interconnections SS-12-001 Privacy in the Workplace
PS-4	Personnel Termination. The organization, upon termination of individual employment: a. Disables information system access within [Assignment: organization-defined time period]; b. Terminates/revokes any authenticators/credentials associated with the individual; c. Conducts exit interviews that include a discussion of [Assignment: organization-defined information security topics]; d. Retrieves all security-related organizational information system-related property; e. Retains access to organizational information and information systems formerly controlled by terminated individual; and f. Notifies [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period].	PS-08-014 Personnel Security

PS-5	Personnel Transfer. The organization: a. Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization; b. Initiates [Assignment: organization-defined transfer or reassignment actions] within [Assignment: organization-defined time period following the formal transfer action]; c. Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and d. Notifies [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period].	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
PS-6	Access Agreements. The organization: a. Develops and documents access agreements for organizational information systems; b. Reviews and updates the access agreements [Assignment: organization-defined frequency]; and c. Ensures that individuals requiring access to organizational information and information systems: 1. Sign appropriate access agreements prior to being granted access; and 2. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or [Assignment: organization-defined frequency].	SS-08-010 Authorization and Access Management
PS-7	Third-Party Personnel Security. The organization: a. Establishes personnel security requirements including security roles and responsibilities for third-party providers; b. Requires third-party providers to comply with personnel security policies and procedures established by the organization; c. Documents personnel security requirements; d. Requires third-party providers to notify [Assignment: organization-defined personnel or roles] of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within [Assignment: organization-defined time period]; and e. Monitors provider compliance.	SS-08-013 Third Party Security Requirements
PS-8	Personnel Sanctions. The organization: a. Employs a formal sanctions process for individuals failing to comply with established information security policies and procedures; and b. Notifies [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-08-014 Personnel Security

Return to: Instructions

Risk Assessment (RA)

NIST #	NIST Control Statement	Applicable State PSG
RA-1	Risk Assessment Policy and Procedures. The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and b. Reviews and updates the current: 1. Risk assessment policy [Assignment: organization-defined frequency]; and 2. Risk assessment procedures [Assignment: organization-defined frequency].	PS-08-031 Information Security - Risk Management SS-08-041 Risk Management Framework
RA-2	Security Categorization. The organization: a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and c. Ensures that the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.	SS-08-041 Risk Management Framework SS-08-014 Data Categorization-Impact Level SS-08-032 System Implementation and Acceptance SM-15-001 Data Steward SS-15-001 Data Storage Location
RA-3	Risk Assessment. The organization: a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; b. Documents risk assessment results in [Selection: security plan; risk assessment report; [Assignment: organization-defined document]]; c. Reviews risk assessment results [Assignment: organization-defined frequency]; d. Disseminates risk assessment results to [Assignment: organization-defined personnel or roles]; and e. Updates the risk assessment [Assignment: organization-defined frequency] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.	PS-08-029 Security Controls Review and Assessments SS-08-042 Independent Security Assessments
RA-4	Risk Assessment Update. [Withdrawn: Incorporated into RA-3].	Withdrawn: Incorporated into RA-3

RA-5	Vulnerability Scanning. The organization: a. Scans for vulnerabilities in the information 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/applications are identified and reported; b. Employs vulnerability scanning 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. Analyzes vulnerability scan reports and results from security control assessments; d. Remediates legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk; and e. Shares information obtained from the vulnerability scanning process and security control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).	PS-08-029 Security Controls Review and Assessments SS-08-042 Independent Security Assessments
RA-6	Technical Surveillance Countermeasures Survey. The organization employs a technical surveillance countermeasures survey at [Assignment: organization-defined locations] [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined events or indicators occur]].	There are no PSGs published for this topic; however, the topic is under review for future PSGs.

Return to: Instructions

System and Services Acquisition (SA)

NIST #	NIST Control Statement	Applicable State PSG
SA-1	System and Services Acquisition Policy and Procedures. The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and b. Reviews and updates the current: 1. System and services acquisition policy [Assignment: organization-defined frequency]; and 2. System and services acquisition procedures [Assignment: organization-defined frequency].	PM-04-002 Acquisition and Use of Telecommunications Services and Equipment PM-06-001 Information Technology Review Policy SM-08-103 Information Technology Review (eAPR) PS-08-011 Third-Party Access SS-08-013 Third-Party Security Requirements SA-14-003 – Requirements to Use Cloud Services SO-10-003 – Enterprise Operational Environment SM-14-008 GTA Endorsement of Proposed Technology Procurement
SA-2	Allocation of Resources. The organization: a. Determines information security requirements for the information system or information system service in mission/business process planning; b. Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process; and c. Establishes a discrete line item for information security in organizational programming and budgeting documentation.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
SA-3	System Development Life Cycle. The organization: a. Manages the information system using [Assignment: organization-defined system development life cycle] that incorporates information security considerations; b. Defines and documents information security roles and responsibilities throughout the system development life cycle; c. Identifies individuals having information security roles and responsibilities; and d. Integrates the organizational information security risk management process into system development life cycle activities.	PS-08-018 Systems and Development Lifecycle SS-08-025 System Lifecycle Management

SA-4	Acquisition Process. The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:
	a. Security functional requirements;
	b. Security strength requirements;
	c. Security assurance requirements;
	d. Security-related documentation requirements;
	e. Requirements for protecting security-related documentation;
	f. Description of the information system development environment and environment in which the system is intended to operate; and
	g. Acceptance criteria.
		PS-08-028 Public Access Systems
		SS-08-013 Third-Party Security Requirements
		SS-08-032 System Implementation and Acceptance
		SA-14-003 – Requirements to Use Cloud Services
		SO-10-003 – Enterprise Operational Environment
		SM-14-008 GTA Endorsement of Proposed Technology Procurement

SA-5	Information System Documentation. The organization: a. Obtains administrator documentation for the information system, system component, or information system service that describes: 1. Secure configuration, installation, and operation of the system, component, or service; 2. Effective use and maintenance of security functions/mechanisms; and 3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; b. Obtains user documentation for the information system, system component, or information system service that describes: 1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms; 2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and 3. User responsibilities in maintaining the security of the system, component, or service; c. Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and [Assignment: organization-defined actions] in response; d. Protects documentation as required, in accordance with the risk management strategy; and e. Distributes documentation to [Assignment: organization-defined personnel or roles].	SS-08-027 System Operations Documentation
SA-6	Software Usage Restrictions. [Withdrawn: Incorporated into CM-10 and SI-7].	Withdrawn: Incorporated into CM-10 and SI-7
SA-7	User-Installed Software. [Withdrawn: Incorporated into CM-11 and SI-7].	Withdrawn: Incorporated into CM-11 and SI-7
SA-8	Security Engineering Principles. The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.	PS-08-020 Separation of Production and Development Environments SS-08-031 Separate Production and Development Environments
SA-9	External Information System Services. The organization: a. Requires that providers of external information system services comply with organizational information security requirements and employ [Assignment: organization-defined security controls] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and c. Employs [Assignment: organization-defined processes, methods, and techniques] to monitor security control compliance by external service providers on an ongoing basis.	PS-08-019 Outsourced Facilities Management SS-08-044 Outsourced IT Services and 3rd Party Interconnections SA-10-009 – Deployment Certification SA-14-003 – Requirements to Use Cloud Services SS-15-001 Data Storage Location

SA-10	Developer Configuration Management. The organization requires the developer of the information system, system component, or information system service to: a. Perform configuration management during system, component, or service [Selection (one or more): design; development; implementation; operation]; 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 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].	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
SA-11	Developer Security Testing and Evaluation. The organization requires the developer of the information system, system component, or information system service to: a. Create and implement a security assessment plan; b. Perform [Selection (one or more): unit; integration; system; regression] testing/evaluation at [Assignment: organization-defined depth and coverage]; c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation; d. Implement a verifiable flaw remediation process; and e. Correct flaws identified during security testing/evaluation.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
SA-12	Supply Chain Protection. The organization protects against supply chain threats to the information system, system component, or information system service by employing [Assignment: organization-defined security safeguards] as part of a comprehensive, defense-in-breadth information security strategy.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
SA-13	Trustworthiness. The organization: a. Describes the trustworthiness required in the [Assignment: organization-defined information system, information system component, or information system service] supporting its critical missions/business functions; and b. Implements [Assignment: organization-defined assurance overlay] to achieve such trustworthiness.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
SA-14	Criticality Analysis. The organization identifies critical information system components and functions by performing a criticality analysis for [Assignment: organization-defined information systems, information system components, or information system services] at [Assignment: organization- defined decision points in the system development life cycle].	There are no PSGs published for this topic; however, the topic is under review for future PSGs.

SA-15	Development Process, Standards, and Tools. The organization: a. Requires the developer of the information system, system component, or information system service to follow a documented development process that: 1. Explicitly addresses security 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. Reviews the development process, standards, tools, and tool options/configurations [Assignment: organization-defined frequency] to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy [Assignment: organization- defined security requirements].	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
SA-16	Developer-Provided Training. The organization requires the developer of the information system, system component, or information system service to provide [Assignment: organization-defined training] on the correct use and operation of the implemented security functions, controls, and/or mechanisms.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
SA-17	Developer Security Architecture and Design. The organization requires the developer of the information system, system component, or information system service to produce a design specification and security architecture that: a. Is consistent with and supportive of the organization’s security architecture which is established within and is an integrated part of the organization’s enterprise architecture; b. Accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components; and c. Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
SA-18	Tamper Resistance and Detection. The organization implements a tamper protection program for the information system, system component, or information system service.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
SA-19	Component Authenticity. The organization: a. Develops and implements anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the information system; and b. Reports counterfeit information system components to [Selection (one or more): source of counterfeit component; [Assignment: organization-defined external reporting organizations]; [Assignment: organization-defined personnel or roles]].	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
SA-20	Customized Development of Critical Components. The organization re-implements or custom develops [Assignment: organization-defined critical information system components].	There are no PSGs published for this topic; however, the topic is under review for future PSGs.

SA-21	Developer Screening. The organization requires that the developer of [Assignment: organization-defined information system, system component, or information system service]: a. Have appropriate access authorizations as determined by assigned [Assignment: organization- defined official government duties]; and b. Satisfy [Assignment: organization-defined additional personnel screening criteria].	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
SA-22	Unsupported System Components. The organization: a. Replaces information system components when support for the components is no longer available from the developer, vendor, or manufacturer; and b. Provides justification and documents approval for the continued use of unsupported system components required to satisfy mission/business needs.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.

Return to: Instructions

System and Communications Protection (SC)

NIST #	NIST Control Statement	Applicable State PSG
SC-1	System and Communications Protection Policy and Procedures. The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and b. Reviews and updates the current: 1. System and communications protection policy [Assignment: organization-defined frequency]; and 2. System and communications protection procedures [Assignment: organization-defined frequency].	PS-08-012 Data and Asset Categorization PS-08-029 Security Controls Review and Assessments SS-08-002 Classification of Personal Information SS-08-014 Data Categorization - Impact Level PS-08-027 Network Security Controls SM-15-001 Data Steward SS-15-001 Data Storage Location
SC-2	Application Partitioning. The information system separates user functionality (including user interface services) from information system management functionality.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
SC-3	Security Function Isolation. The information system isolates security functions from non-security functions.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
SC-4	Information in Shared Resources. The information system prevents unauthorized and unintended information transfer via shared system resources.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
SC-5	Denial of Service Protection. The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or reference to source for such information] by employing [Assignment: organization-defined security safeguards].	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
SC-6	Resource Availability. The information system protects the availability of resources by allocating [Assignment: organization-defined resources] by [Selection (one or more); priority; quota; [Assignment: organization-defined security safeguards]].	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
SC-7	Boundary Protection. The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements sub-networks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.	PS-08-027 Network Security Controls PS-08-030 Network Security - Information Flow SS-08-047 Network Security - Boundary Protection
SC-8	Transmission Confidentiality and Integrity. The information system protects the [Selection (one or more): confidentiality; integrity] of transmitted information.	PM-07-003 Statewide Data Sharing PS-08-030 Network Security - Information Flow
SC-9	Transmission Confidentiality. [Withdrawn: Incorporated into SC-8].	Withdrawn: Incorporated into SC-8

SC-10	Network Disconnect. The information system terminates the network connection associated with a communications session at the end of the session or after [Assignment: organization-defined time period] of inactivity.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
SC-11	Trusted Path. The information system establishes a trusted communications path between the user and the following security functions of the system: [Assignment: organization-defined security functions to include at a minimum, information system authentication and re-authentication].	PM-07-003 Statewide Data Sharing PS-08-012 Data and Asset Categorization PS-08-024 Use of Cryptography SS-08-040 Cryptographic Controls
SC-12	Cryptographic Key Establishment and Management. The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].	PS-08-024 Use of Cryptography
SC-13	Cryptographic Protection. The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	PS-08-024 Use of Cryptography
SC-14	Public Access Protections. [Withdrawn: Capability provided by AC-2, AC-3, AC-5, AC-6, SI-3, SI-4, SI-5, SI-7, SI-10].	Withdrawn: Capability provided by AC-2, AC-3, AC-5, AC-6, SI-3, SI-4, SI-5, SI-7, SI-10
SC-15	Collaborative Computing Devices. The information system: a. Prohibits remote activation of collaborative computing devices with the following exceptions: [Assignment: organization-defined exceptions where remote activation is to be allowed]; and b. Provides an explicit indication of use to users physically present at the devices.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
SC-16	Transmission of Security Attributes. The information system associates [Assignment: organization-defined security attributes] with information exchanged between information systems and between system components.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
SC-17	Public Key Infrastructure Certificates. The organization issues public key certificates under an [Assignment: organization- defined certificate policy] or obtains public key certificates from an approved service provider.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
SC-18	Mobile Code. The organization: a. Defines acceptable and unacceptable mobile code and mobile code technologies; b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and c. Authorizes, monitors, and controls the use of mobile code within the information system.	PS-08-021 Protection from Malicious Software PS-08-028 Public Access Systems SS-08-033 Malicious Code Incident Prevention
SC-19	Voice Over Internet Protocol. The organization: a. Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and b. Authorizes, monitors, and controls the use of VoIP within the information system.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.

SC-20	Secure Name /Address Resolution Service (Authoritative Source). The information system: a. Provides additional data origin and integrity artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and b. Provides 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.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver). The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
SC-22	Architecture and Provisioning for Name/Address Resolution Service. The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
SC-23	Session Authenticity. The information system protects the authenticity of communications sessions.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
SC-24	Fail in Known State. The information system fails to a [Assignment: organization-defined known-state] for [Assignment: organization-defined types of failures] preserving [Assignment: organization-defined system state information] in failure.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
SC-25	Thin Nodes. The organization employs [Assignment: organization-defined information system components] with minimal functionality and information storage.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
SC-26	Honeypots. The information system includes components specifically designed to be the target of malicious attacks for the purpose of detecting, deflecting, and analyzing such attacks.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
SC-27	Platform-Independent Applications. The information system includes: [Assignment: organization-defined platform- independent applications].	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
SC-28	Protection of Information at Rest. The information system protects the [Selection (one or more): confidentiality; integrity] of [Assignment: organization-defined information at rest].	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
SC-29	Heterogeneity. The organization employs a diverse set of information technologies for [Assignment: organization-defined information system components] in the implementation of the information system.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
SC-30	Concealment and Misdirection. The organization employs [Assignment: organization-defined concealment and misdirection techniques] for [Assignment: organization-defined information systems] at [Assignment: organization-defined time periods] to confuse and mislead adversaries.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
SC-31	Covert Channel Analysis. The organization: a. Performs a covert channel analysis to identify those aspects of communications within the information system that are potential avenues for covert [Selection (one or more): storage; timing] channels; and b. Estimates the maximum bandwidth of those channels.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.

SC-32	Information System Partitioning. The organization partitions the information system into [Assignment: organization-defined information system components] residing in separate physical domains or environments based on [Assignment: organization-defined circumstances for physical separation of components].	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
SC-33	Transmission Preparation Integrity. [Withdrawn: Incorporated into SC-8].	Withdrawn: Incorporated into SC-8
SC-34	Non-Modifiable Executable Programs. The information system at [Assignment: organization-defined information system components]: a. Loads and executes the operating environment from hardware-enforced, read-only media; and b. Loads and executes [Assignment: organization-defined applications] from hardware- enforced, read-only media.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
SC-35	Honeyclients. The information system includes components that proactively seek to identify malicious websites and/or web-based malicious code.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
SC-36	Distributed Processing and Storage. The organization distributes [Assignment: organization-defined processing and storage] across multiple physical locations.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
SC-37	Out-of-Band Channels. The organization employs [Assignment: organization-defined out-of-band channels] for the physical delivery or electronic transmission of [Assignment: organization-defined information, information system components, or devices] to [Assignment: organization-defined individuals or information systems].	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
SC-38	Operations Security. The organization employs [Assignment: organization-defined operations security safeguards] to protect key organizational information throughout the system development life cycle.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
SC-39	Process Isolation. The information system maintains a separate execution domain for each executing process.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
SC-40	Wireless Link Protection. The information system protects external and internal [Assignment: organization-defined wireless links] from [Assignment: organization-defined types of signal parameter attacks or references to sources for such attacks].	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
SC-41	Port and I/O Device Access. The organization physically disables or removes [Assignment: organization-defined connection ports or input/output devices] on [Assignment: organization-defined information systems or information system components].	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
SC-42	Sensor Capability and Data. The information system: a. Prohibits the remote activation of environmental sensing capabilities with the following exceptions: [Assignment: organization-defined exceptions where remote activation of sensors is allowed]; and b. Provides an explicit indication of sensor use to [Assignment: organization-defined class of users].	There are no PSGs published for this topic; however, the topic is under review for future PSGs.

SC-43	Usage Restrictions. The organization: a. Establishes usage restrictions and implementation guidance for [Assignment: organization- defined information system components] based on the potential to cause damage to the information system if used maliciously; and b. Authorizes, monitors, and controls the use of such components within the information system.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
SC-44	Detonation Chambers. The organization employs a detonation chamber capability within [Assignment: organization-defined information system, system component, or location].	There are no PSGs published for this topic; however, the topic is under review for future PSGs.

Return to: Instructions

System and Information Integrity (SI)

NIST#	NIST Control Statement	Applicable State PSG
SI-1	System and Information Integrity Policy and Procedures. The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and b. Reviews and updates the current: 1. System and information integrity policy [Assignment: organization-defined frequency]; and 2. System and information integrity procedures [Assignment: organization-defined frequency].	PS-08-007 Reliance on Electronic Records SS-08-003 Data Security - Electronic Records
SI-2	Flaw Remediation. The organization: a. Identifies, reports, and corrects information system flaws; b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; c. Installs security-relevant software and firmware updates within [Assignment: organization- defined time period] of the release of the updates; and d. Incorporates flaw remediation into the organizational configuration management process.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
SI-3	Malicious Code Protection. The organization: a. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code; b. Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures; c. Configures malicious code protection mechanisms to: 1. Perform periodic scans of the information system [Assignment: organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more); endpoint; network entry/exit points] as the files are downloaded, opened, or executed in accordance with organizational security policy; and 2. [Selection (one or more): block malicious code; quarantine malicious code; send alert to administrator; [Assignment: organization-defined action]] in response to malicious code detection; and d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.	PS-08-021 Protection from Malicious Software PS-08-028 Public Access Systems SS-08-033 Malicious Code Incident Prevention

SI-4	Information System Monitoring. The organization: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization- defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization- defined techniques and methods]; c. Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization; d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion; e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and g. Provides [Assignment: organization-defined information system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].	SS-08-003 Data Security - Electronic Records PS-08-027 Network Security Controls PS-08-022 Security Log Management PS-08-023 Remote Access SS-08-038 Secure Remote Access PS-08-030 Network Security - Information Flow SS-08-039 Wireless and Mobile Computing SS-08-044 Outsourced IT Services and Third-Party Interconnections SS-08-047 Network Security - Boundary Protection SS-08-048 Network Access and Session Controls SS-08-049 Web and E-Commerce Security SS-15-001 Data Storage Location
SI-5	Security Alerts, Advisories, and Directives. The organization: a. Receives information system security alerts, advisories, and directives from [Assignment: organization-defined external organizations] on an ongoing basis; b. Generates internal security alerts, advisories, and directives as deemed necessary; c. Disseminates 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. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
SI-6	Security Function Verification. The information system: a. Verifies the correct operation of [Assignment: organization-defined security functions]; b. Performs this verification [Selection (one or more): [Assignment: organization-defined system transitional states]; upon command by user with appropriate privilege; [Assignment: organization-defined frequency]]; c. Notifies [Assignment: organization-defined personnel or roles] of failed security verification tests; and d. [Selection (one or more): shuts the information system down; restarts the information system; [Assignment: organization-defined alternative action(s)]] when anomalies are discovered.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.

SI-7	Software, Firmware, and Information Integrity. The organization employs integrity verification tools to detect unauthorized changes to [Assignment: organization-defined software, firmware, and information].	PS-08-007 Reliance on Electronic Records SS-08-003 Data Security - Electronic Records PS-08-028 Public Access Systems PS-08-021 Protection from Malicious Software SS-08-033 Malicious Code Incident Prevention
SI-8	Spam Protection. The organization: a. Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and b. Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.	PS-08-021 Protection from Malicious Software PS-08-028 Public Access Systems SS-08-033 Malicious Code Incident Prevention
SI-9	Information Input Restrictions. [Withdrawn: Incorporated into AC-2, AC-3, AC-5, AC-6].	Withdrawn: Incorporated into AC-2, AC-3, AC-5, AC-6
SI-10	Information Input Validation. The information system checks the validity of [Assignment: organization-defined information inputs].	PS-08-007 Reliance on Electronic Records SS-08-003 Data Security - Electronic Records PS-08-028 Public Access Systems
SI-11	Error Handling. The information system: a. Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and b. Reveals error messages only to [Assignment: organization-defined personnel or roles].	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
SI-12	Information Handling and Retention. The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
SI-13	Predictable Failure Prevention. The organization: a. Determines mean time to failure (MTTF) for [Assignment: organization-defined information system components] in specific environments of operation; and b. Provides substitute information system components and a means to exchange active and standby components at [Assignment: organization-defined MTTF substitution criteria].	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
SI-14	Non-Persistence. The organization implements non-persistent [Assignment: organization-defined information system components and services] that are initiated in a known state and terminated [Selection (one or more): upon end of session of use; periodically at [Assignment: organization- defined frequency]].	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
SI-15	Information Output Filtering. The information system validates information output from [Assignment: organization- defined software programs and/or applications] to ensure that the information is consistent with the expected content.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.
SI-16	Memory Protection. The information system implements [Assignment: organization-defined security safeguards] to protect its memory from unauthorized code execution.	There are no PSGs published for this topic; however, the topic is under review for future PSGs.

SI-17	Fail-Safe Procedures. The information system implements [Assignment: organization-defined fail-safe procedures] when [Assignment: organization-defined failure conditions occur].	There are no PSGs published for this topic; however, the topic is under review for future PSGs.

Return to: Instructions