NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference docume Secure Controls Framework (SCF) version 2026.1
STRM Guidance: https://securecontrolsframework.com/set-theory-relationship-mapping-strm/

Focal Document: **NIST SP 800-53 Rev 5.2 Security and Privacy Controls for Information Systems and Organizations**
Focal Document U https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final
Published STRM U https://content.securecontrolsframework.com/strm/scf-strm-general-nist-800-53-r5-2.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Relationsh	Notes	NIST SP 800-53B Baseline
AC-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] access control policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the access control policy and the associated access controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the access control policy and procedures; andc. Review and update the current access control:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5		Low
AC-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] access control policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the access control policy and the associated access controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the access control policy and procedures; andc. Review and update the current access control:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5		Low
AC-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] access control policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the access control policy and the associated access controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the access control policy and procedures; andc. Review and update the current access control:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10		Low
AC-02	Account Management	a. Define and document the types of accounts allowed and specifically prohibited for use within the system;b. Assign account managers;c. Require [Assignment: organization-defined prerequisites and criteria] for group and role membership;d. Specify:1. Authorized users of the system;2. Group and role membership; and3. Access authorizations (i.e., privileges) and [Assignment: organization-defined attributes (as required)] for each account;e. Require approvals by [Assignment: organization-defined personnel or roles] for requests to create accounts;f. Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, prerequisites, and criteria];g. Monitor the use of accounts;h. Notify account managers and [Assignment: organization-defined personnel or roles] within:1. [Assignment: organization-defined time period] when accounts are no longer required;2. [Assignment: organization-defined time period] when users are terminated or transferred; and3. [Assignment: organization-defined time period] when system usage or need-to-know changes for an individual;i. Authorize access to the system based on:1. A valid access authorization;2. Intended system usage; and3. [Assignment: organization-defined attributes (as required)];j. Review accounts for compliance with account management requirements [Assignment: organization-defined frequency];k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; andl. Align account management processes with personnel termination and transfer processes.	Functional	Intersects With	Termination of Employment	IAC-07.2	Mechanisms exist to revoke user access rights in a timely manner, upon termination of employment or contract.	5		Low
AC-02	Account Management	a. Define and document the types of accounts allowed and specifically prohibited for use within the system;b. Assign account managers;c. Require [Assignment: organization-defined prerequisites and criteria] for group and role membership;d. Specify:1. Authorized users of the system;2. Group and role membership; and3. Access authorizations (i.e., privileges) and [Assignment: organization-defined attributes (as required)] for each account;e. Require approvals by [Assignment: organization-defined personnel or roles] for requests to create accounts;f. Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, prerequisites, and criteria];g. Monitor the use of accounts;h. Notify account managers and [Assignment: organization-defined personnel or roles] within:1. [Assignment: organization-defined time period] when accounts are no longer required;2. [Assignment: organization-defined time period] when users are terminated or transferred; and3. [Assignment: organization-defined time period] when system usage or need-to-know changes for an individual;i. Authorize access to the system based on:1. A valid access authorization;2. Intended system usage; and3. [Assignment: organization-defined attributes (as required)];j. Review accounts for compliance with account management requirements [Assignment: organization-defined frequency];k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; andl. Align account management processes with personnel termination and transfer processes.	Functional	Intersects With	Account Management	IAC-15	Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.	5		Low

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-53B Baseline
AC-02	Account Management	a. Define and document the types of accounts allowed and specifically prohibited for use within the system;b. Assign account managers;c. Require [Assignment: organization-defined prerequisites and criteria] for group and role membership;d. Specify:1. Authorized users of the system;2. Group and role membership; and3. Access authorizations (i.e., privileges) and [Assignment: organization-defined attributes (as required)] for each account;e. Require approvals by [Assignment: organization-defined personnel or roles] for requests to create accounts;f. Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, prerequisites, and criteria];g. Monitor the use of accounts;h. Notify account managers and [Assignment: organization-defined personnel or roles] within:1. [Assignment: organization-defined time period] when accounts are no longer required;2. [Assignment: organization-defined time period] when users are terminated or transferred; and3. [Assignment: organization-defined time period] when system usage or need-to-know changes for an individual;i. Authorize access to the system based on:1. A valid access authorization;2. Intended system usage; and3. [Assignment: organization-defined attributes (as required)];j. Review accounts for compliance with account management requirements [Assignment: organization-defined frequency];k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; andl. Align account management processes with personnel termination and transfer processes.	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5		Low
AC-02	Account Management	a. Define and document the types of accounts allowed and specifically prohibited for use within the system;b. Assign account managers;c. Require [Assignment: organization-defined prerequisites and criteria] for group and role membership;d. Specify:1. Authorized users of the system;2. Group and role membership; and3. Access authorizations (i.e., privileges) and [Assignment: organization-defined attributes (as required)] for each account;e. Require approvals by [Assignment: organization-defined personnel or roles] for requests to create accounts;f. Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, prerequisites, and criteria];g. Monitor the use of accounts;h. Notify account managers and [Assignment: organization-defined personnel or roles] within:1. [Assignment: organization-defined time period] when accounts are no longer required;2. [Assignment: organization-defined time period] when users are terminated or transferred; and3. [Assignment: organization-defined time period] when system usage or need-to-know changes for an individual;i. Authorize access to the system based on:1. A valid access authorization;2. Intended system usage; and3. [Assignment: organization-defined attributes (as required)];j. Review accounts for compliance with account management requirements [Assignment: organization-defined frequency];k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; andl. Align account management processes with personnel termination and transfer processes.	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-12	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.	5		Low
AC-02(01)	Account Management | Automated System Account Management	Support the management of system accounts using [Assignment: organization-defined automated mechanisms].	Functional	Intersects With	Automated System Account Management (Directory Services)	IAC-15.1	Automated mechanisms exist to support the management of system accounts (e.g., directory services).	5		Moderate
AC-02(02)	Account Management | Automated Temporary and Emergency Account Management	Automatically [Selection (one): remove; disable] temporary and emergency accounts after [Assignment: organization-defined time period for each type of account].	Functional	Equal	Removal of Temporary / Emergency Accounts	IAC-15.2	Automated mechanisms exist to disable or remove temporary and emergency accounts after an organization-defined time period for each type of account.	10		Moderate
AC-02(03)	Account Management | Disable Accounts	Disable accounts within [Assignment: organization-defined time period] when the accounts:a. Have expired;b. Are no longer associated with a user or individual;c. Are in violation of organizational policy; ord. Have been inactive for [Assignment: organization-defined time period].	Functional	Equal	Disable Inactive Accounts	IAC-15.3	Automated mechanisms exist to disable inactive accounts after an organization-defined time period.	10		Moderate
AC-02(04)	Account Management | Automated Audit Actions	Automatically audit account creation, modification, enabling, disabling, and removal actions.	Functional	Equal	Automated Audit Actions	IAC-15.4	Automated mechanisms exist to audit account creation, modification, enabling, disabling and removal actions and notify organization-defined personnel or roles.	10		Moderate
AC-02(05)	Account Management | Inactivity Logout	Require that users log out when [Assignment: organization-defined time period of expected inactivity or description of when to log out].	Functional	Equal	Session Lock	IAC-24	Mechanisms exist to initiate a session lock after an organization-defined time period of inactivity, or upon receiving a request from a user and retain the session lock until the user reestablishes access using established identification and authentication methods.	10		Moderate
AC-02(06)	Account Management | Dynamic Privilege Management	Implement [Assignment: organization-defined dynamic privilege management capabilities].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
AC-02(07)	Account Management | Privileged User Accounts	a. Establish and administer privileged user accounts in accordance with [Selection (one): a role-based access scheme; an attribute-based access scheme];b. Monitor privileged role or attribute assignments;c. Monitor changes to roles or attributes; andd. Revoke access when privileged role or attribute assignments are no longer appropriate.	Functional	Equal	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	10		Not Selected
AC-02(08)	Account Management | Dynamic Account Management	Create, activate, manage, and deactivate [Assignment: organization-defined system accounts] dynamically.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
AC-02(09)	Account Management | Restrictions on Use of Shared and Group Accounts	Only permit the use of shared and group accounts that meet [Assignment: organization-defined conditions for establishing shared and group accounts].	Functional	Equal	Restrictions on Shared Groups / Accounts	IAC-15.5	Mechanisms exist to authorize the use of shared/group accounts only under certain organization-defined conditions.	10		Not Selected
AC-02(10)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
AC-02(11)	Account Management | Usage Conditions	Enforce [Assignment: organization-defined circumstances and/or usage conditions] for [Assignment: organization-defined system accounts].	Functional	Equal	Usage Conditions	IAC-15.8	Automated mechanisms exist to enforce usage conditions for users and/or roles.	10		High
AC-02(12)	Account Management | Account Monitoring for Atypical Usage	a. Monitor system accounts for [Assignment: organization-defined atypical usage]; andb. Report atypical usage of system accounts to [Assignment: organization-defined personnel or roles].	Functional	Equal	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	10		High
AC-02(13)	Account Management | Disable Accounts for High-risk Individuals	Disable accounts of individuals within [Assignment: organization-defined time period] of discovery of [Assignment: organization-defined significant risks].	Functional	Intersects With	High-Risk Terminations	HRS-09.2	Mechanisms exist to expedite the process of removing "high risk" individual's access to Technology Assets, Applications, Services and/or Data (TAASD) upon termination, as determined by management.	5		Moderate
AC-02(13)	Account Management | Disable Accounts for High-risk Individuals	Disable accounts of individuals within [Assignment: organization-defined time period] of discovery of [Assignment: organization-defined significant risks].	Functional	Intersects With	Account Disabling for High Risk Individuals	IAC-15.6	Mechanisms exist to disable accounts immediately upon notification for users posing a significant risk to the organization.	5		Moderate
AC-03	Access Enforcement	Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	Functional	Intersects With	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	5		Low

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-53B Baseline
AC-03	Access Enforcement	Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-12	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.	5		Low
AC-03	Access Enforcement	Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5		Low
AC-03(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
AC-03(02)	Access Enforcement | Dual Authorization	Enforce dual authorization for [Assignment: organization-defined privileged commands and/or other organization-defined actions].	Functional	Intersects With	Two-Person Rule	HRS-12.1	Mechanisms exist to enforce a two-person rule for implementing changes to sensitive Technology Assets, Applications and/or Services (TAAS).	5		Not Selected
AC-03(02)	Access Enforcement | Dual Authorization	Enforce dual authorization for [Assignment: organization-defined privileged commands and/or other organization-defined actions].	Functional	Intersects With	Dual Authorization for Privileged Commands	IAC-20.5	Automated mechanisms exist to enforce dual authorization for privileged commands.	5		Not Selected
AC-03(03)	Access Enforcement | Mandatory Access Control	Enforce [Assignment: organization-defined mandatory access control policy] over the set of covered subjects and objects specified in the policy, and where the policy:a. Is uniformly enforced across the covered subjects and objects within the system;b. Specifies that a subject that has been granted access to information is constrained from doing any of the following;1. Passing the information to unauthorized subjects or objects;2. Granting its privileges to other subjects;3. Changing one or more security attributes (specified by the policy) on subjects, objects, the system, or system components;4. Choosing the security attributes and attribute values (specified by the policy) to be associated with newly created or modified objects; and5. Changing the rules governing access control; andc. Specifies that [Assignment: organization-defined subjects] may explicitly be granted [Assignment: organization-defined privileges] such that they are not limited by any defined subset (or all) of the above constraints.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
AC-03(04)	Access Enforcement | Discretionary Access Control	Enforce [Assignment: organization-defined discretionary access control policy] over the set of covered subjects and objects specified in the policy, and where the policy specifies that a subject that has been granted access to information can do one or more of the following:a. Pass the information to any other subjects or objects;b. Grant its privileges to other subjects;c. Change security attributes on subjects, objects, the system, or the system's components;d. Choose the security attributes to be associated with newly created or revised objects; ore. Change the rules governing access control.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
AC-03(05)	Access Enforcement | Security-relevant Information	Prevent access to [Assignment: organization-defined security-relevant information] except during secure, non-operable system states.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
AC-03(06)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
AC-03(07)	Access Enforcement | Role-based Access Control	Enforce a role-based access control policy over defined subjects and objects and control access based upon [Assignment: organization-defined roles and users authorized to assume such roles].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
AC-03(08)	Access Enforcement | Revocation of Access Authorizations	Enforce the revocation of access authorizations resulting from changes to the security attributes of subjects and objects based on [Assignment: organization-defined rules governing the timing of revocations of access authorizations].	Functional	Equal	Revocation of Access Authorizations	IAC-20.6	Mechanisms exist to revoke logical and physical access authorizations.	10		Not Selected
AC-03(09)	Access Enforcement | Controlled Release	Release information outside of the system only if:a. The receiving [Assignment: organization-defined system or system component] provides [Assignment: organization-defined controls]; andb. [Assignment: organization-defined controls] are used to validate the appropriateness of the information designated for release.	Functional	Equal	Controlled Release	DCH-03.3	Automated mechanisms exist to validate cybersecurity and data protection attributes prior to releasing information to external Technology Assets, Applications and/or Services (TAAS).	10		Not Selected
AC-03(10)	Access Enforcement | Audited Override of Access Control Mechanisms	Employ an audited override of automated access control mechanisms under [Assignment: organization-defined conditions] by [Assignment: organization-defined roles].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
AC-03(11)	Access Enforcement | Restrict Access to Specific Information Types	Restrict access to data repositories containing [Assignment: organization-defined information types].	Functional	Equal	Sensitive / Regulated Data Access Enforcement	CFG-08	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to restrict access to sensitive/regulated data.	10		Not Selected
AC-03(12)	Access Enforcement | Assert and Enforce Application Access	a. Require applications to assert, as part of the installation process, the access needed to the following system applications and functions: [Assignment: organization-defined system applications and functions];b. Provide an enforcement mechanism to prevent unauthorized access; andc. Approve access changes after initial installation of the application.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
AC-03(13)	Access Enforcement | Attribute-based Access Control	Enforce attribute-based access control policy over defined subjects and objects and control access based upon [Assignment: organization-defined attributes to assume access permissions].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
AC-03(14)	Access Enforcement | Individual Access	Provide [Assignment: organization-defined mechanisms] to enable individuals to have access to the following elements of their personally identifiable information: [Assignment: organization-defined elements].	Functional	Equal	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request erasure of their PD; and (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	10		Not Selected
AC-03(15)	Access Enforcement | Discretionary and Mandatory Access Control	a. Enforce [Assignment: organization-defined mandatory access control policy] over the set of covered subjects and objects specified in the policy; andb. Enforce [Assignment: organization-defined discretionary access control policy] over the set of covered subjects and objects specified in the policy.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
AC-04	Information Flow Enforcement	Enforce approved authorizations for controlling the flow of information within the system and between connected systems based on [Assignment: organization-defined information flow control policies].	Functional	Equal	Data Flow Enforcement – Access Control Lists (ACLs)	NET-04	Mechanisms exist to implement and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restrict network traffic to only what is authorized.	10		Moderate
AC-04(01)	Information Flow Enforcement | Object Security and Privacy Attributes	Use [Assignment: organization-defined security and privacy attributes] associated with [Assignment: organization-defined information, source, and destination objects] to enforce [Assignment: organization-defined information flow control policies] as a basis for flow control decisions.	Functional	Equal	Object Security Attributes	NET-04.2	Mechanisms exist to associate security attributes with information, source and destination objects to enforce defined information flow control configurations as a basis for flow control decisions.	10		Not Selected
AC-04(02)	Information Flow Enforcement | Processing Domains	Use protected processing domains to enforce [Assignment: organization-defined information flow control policies] as a basis for flow control decisions.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-53B Baseline
AC-04(03)	Information Flow Enforcement | Dynamic Information Flow Control	Enforce [Assignment: organization-defined information flow control policies].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
AC-04(04)	Information Flow Enforcement | Flow Control of Encrypted Information	Prevent encrypted information from bypassing [Assignment: organization-defined information flow control mechanisms] by [Selection (one or more): decrypting the information; blocking the flow of the encrypted information; terminating communications sessions attempting to pass encrypted information; [Assignment: organization-defined procedure or method]]	Functional	Equal	Content Check for Encrypted Data	NET-04.3	Mechanisms exist to prevent encrypted data from bypassing content-checking mechanisms.	10		High
AC-04(05)	Information Flow Enforcement | Embedded Data Types	Enforce [Assignment: organization-defined limitations] on embedding data types within other data types.	Functional	Equal	Embedded Data Types	NET-04.4	Mechanisms exist to enforce limitations on embedding data within other data types.	10		Not Selected
AC-04(06)	Information Flow Enforcement | Metadata	Enforce information flow control based on [Assignment: organization-defined metadata].	Functional	Equal	Metadata	NET-04.5	Mechanisms exist to enforce information flow controls based on metadata.	10		Not Selected
AC-04(07)	Information Flow Enforcement | One-way Flow Mechanisms	Enforce one-way information flows through hardware-based flow control mechanisms.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
AC-04(08)	Information Flow Enforcement | Security and Privacy Policy Filters	a. Enforce information flow control using [Assignment: organization-defined security or privacy policy filters] as a basis for flow control decisions for [Assignment: organization-defined information flows]; andb. [Selection (one or more): Block; Strip; Modify; Quarantine] data after a filter processing failure in accordance with [Assignment: organization-defined security or privacy policy].	Functional	Equal	Policy Decision Point (PDP)	NET-04.7	Automated mechanisms exist to evaluate access requests against established criteria to dynamically and uniformly enforce access rights and permissions.	10		Not Selected
AC-04(09)	Information Flow Enforcement | Human Reviews	Enforce the use of human reviews for [Assignment: organization-defined information flows] under the following conditions: [Assignment: organization-defined conditions].	Functional	Equal	Human Reviews	NET-04.6	Mechanisms exist to enforce the use of human reviews for Access Control Lists (ACLs) and similar rulesets on a routine basis.	10		Not Selected
AC-04(10)	Information Flow Enforcement | Enable and Disable Security or Privacy Policy Filters	Provide the capability for privileged administrators to enable and disable [Assignment: organization-defined security or privacy policy filters] under the following conditions: [Assignment: organization-defined conditions].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
AC-04(11)	Information Flow Enforcement | Configuration of Security or Privacy Policy Filters	Provide the capability for privileged administrators to configure [Assignment: organization-defined security or privacy policy filters] to support different security or privacy policies.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
AC-04(12)	Information Flow Enforcement | Data Type Identifiers	When transferring information between different security domains, use [Assignment: organization-defined data type identifiers] to validate data essential for information flow decisions.	Functional	Equal	Data Type Identifiers	NET-04.8	Automated mechanisms exist to utilize data type identifiers to validate data essential for information flow decisions when transferring information between different security domains.	10		Not Selected
AC-04(13)	Information Flow Enforcement | Decomposition into Policy-relevant Subcomponents	When transferring information between different security domains, decompose information into [Assignment: organization-defined policy-relevant subcomponents] for submission to policy enforcement mechanisms.	Functional	Equal	Decomposition Into Policy-Related Subcomponents	NET-04.9	Automated mechanisms exist to decompose information into policy-relevant subcomponents for submission to policy enforcement mechanisms, when transferring information between different security domains.	10		Not Selected
AC-04(14)	Information Flow Enforcement | Security or Privacy Policy Filter Constraints	When transferring information between different security domains, implement [Assignment: organization-defined security or privacy policy filters] requiring fully enumerated formats that restrict data structure and content.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
AC-04(15)	Information Flow Enforcement | Detection of Unsanctioned Information	When transferring information between different security domains, examine the information for the presence of [Assignment: organization-defined unsanctioned information] and prohibit the transfer of such information in accordance with the [Assignment: organization-defined security or privacy policy].	Functional	Equal	Detection of Unsanctioned Information	NET-04.10	Automated mechanisms exist to implement security policy filters requiring fully enumerated formats that restrict data structure and content, when transferring information between different security domains.	10		Not Selected
AC-04(16)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
AC-04(17)	Information Flow Enforcement | Domain Authentication	Uniquely identify and authenticate source and destination points by [Selection (one or more): organization; system; application; service; individual] for information transfer.	Functional	Equal	Cross Domain Authentication	NET-04.12	Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.	10		Not Selected
AC-04(18)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
AC-04(19)	Information Flow Enforcement | Validation of Metadata	When transferring information between different security domains, implement [Assignment: organization-defined security or privacy policy filters] on metadata.	Functional	Equal	Metadata Validation	NET-04.13	Automated mechanisms exist to apply cybersecurity and/or data protection filters on metadata.	10		Not Selected
AC-04(20)	Information Flow Enforcement | Approved Solutions	Employ [Assignment: organization-defined solutions in approved configurations] to control the flow of [Assignment: organization-defined information] across security domains.	Functional	Equal	Approved Solutions	NET-04.11	Automated mechanisms exist to examine information for the presence of unsanctioned information and prohibits the transfer of such information, when transferring information between different security domains.	10		Not Selected
AC-04(21)	Information Flow Enforcement | Physical or Logical Separation of Information Flows	Separate information flows logically or physically using [Assignment: organization-defined mechanisms and/or techniques] to accomplish [Assignment: organization-defined required separations by types of information].	Functional	Equal	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate Technology Assets, Applications and/or Services (TAAS) to protect from other network resources.	10		Not Selected
AC-04(22)	Information Flow Enforcement | Access Only	Provide access from a single device to computing platforms, applications, or data residing in multiple different security domains, while preventing information flow between the different security domains.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
AC-04(23)	Information Flow Enforcement | Modify Non-releasable Information	When transferring information between different security domains, modify non-releasable information by implementing [Assignment: organization-defined modification action].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
AC-04(24)	Information Flow Enforcement | Internal Normalized Format	When transferring information between different security domains, parse incoming data into an internal normalized format and regenerate the data to be consistent with its intended specification.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
AC-04(25)	Information Flow Enforcement | Data Sanitization	When transferring information between different security domains, sanitize data to minimize [Selection (one or more): delivery of malicious content, command and control of malicious code, malicious code augmentation, and steganography encoded data; spillage of sensitive information] in accordance with [Assignment: organization-defined policy].	Functional	Equal	Personal Data (PD) Retention & Disposal	PRI-05	Mechanisms exist to: (1) Retain Personal Data (PD), including metadata, for an organization-defined time period to fulfill the purpose(s) identified in the notice or as required by law; (2) Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of storage; and (3) Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived records).	10		Not Selected
AC-04(26)	Information Flow Enforcement | Audit Filtering Actions	When transferring information between different security domains, record and audit content filtering actions and results for the information being filtered.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
AC-04(27)	Information Flow Enforcement | Redundant/independent Filtering Mechanisms	When transferring information between different security domains, implement content filtering solutions that provide redundant and independent filtering mechanisms for each data type.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
AC-04(28)	Information Flow Enforcement | Linear Filter Pipelines	When transferring information between different security domains, implement a linear content filter pipeline that is enforced with discretionary and mandatory access controls.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-53B Baseline
AC-04(29)	Information Flow Enforcement | Filter Orchestration Engines	When transferring information between different security domains, employ content filter orchestration engines to ensure that:a. Content filtering mechanisms successfully complete execution without errors; andb. Content filtering actions occur in the correct order and comply with [Assignment: organization-defined policy].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
AC-04(30)	Information Flow Enforcement | Filter Mechanisms Using Multiple Processes	When transferring information between different security domains, implement content filtering mechanisms using multiple processes.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
AC-04(31)	Information Flow Enforcement | Failed Content Transfer Prevention	When transferring information between different security domains, prevent the transfer of failed content to the receiving domain.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
AC-04(32)	Information Flow Enforcement | Process Requirements for Information Transfer	When transferring information between different security domains, the process that transfers information between filter pipelines:a. Does not filter message content;b. Validates filtering metadata;c. Ensures the content associated with the filtering metadata has successfully completed filtering; andd. Transfers the content to the destination filter pipeline.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
AC-05	Separation of Duties	a. Identify and document [Assignment: organization-defined duties of individuals requiring separation]; andb. Define system access authorizations to support separation of duties.	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5		Moderate
AC-05	Separation of Duties	a. Identify and document [Assignment: organization-defined duties of individuals requiring separation]; andb. Define system access authorizations to support separation of duties.	Functional	Intersects With	Dual Authorization for Change	CHG-04.3	Mechanisms exist to enforce a two-person rule for implementing changes to critical Technology Assets, Applications and/or Services (TAAS).	5		Moderate
AC-05	Separation of Duties	a. Identify and document [Assignment: organization-defined duties of individuals requiring separation]; andb. Define system access authorizations to support separation of duties.	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-12	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.	5		Moderate
AC-05	Separation of Duties	a. Identify and document [Assignment: organization-defined duties of individuals requiring separation]; andb. Define system access authorizations to support separation of duties.	Functional	Intersects With	Separation of Duties (SoD)	HRS-11	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	5		Moderate
AC-06	Least Privilege	Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.	Functional	Intersects With	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5		Moderate
AC-06	Least Privilege	Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.	Functional	Intersects With	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	5		Moderate
AC-06(01)	Least Privilege | Authorize Access to Security Functions	Authorize access for [Assignment: organization-defined individuals or roles] to:a. [Assignment: organization-defined security functions (deployed in hardware, software, and firmware)]; andb. [Assignment: organization-defined security-relevant information].	Functional	Equal	Authorize Access to Security Functions	IAC-21.1	Mechanisms exist to limit access to security functions to explicitly-authorized privileged users.	10		Moderate
AC-06(02)	Least Privilege | Non-privileged Access for Nonsecurity Functions	Require that users of system accounts (or roles) with access to [Assignment: organization-defined security functions or security-relevant information] use non-privileged accounts or roles, when accessing nonsecurity functions.	Functional	Equal	Non-Privileged Access for Non-Security Functions	IAC-21.2	Mechanisms exist to prohibit privileged users from using privileged accounts, while performing non-security functions.	10		Moderate
AC-06(03)	Least Privilege | Network Access to Privileged Commands	Authorize network access to [Assignment: organization-defined privileged commands] only for [Assignment: organization-defined compelling operational needs] and document the rationale for such access in the security plan for the system.	Functional	Equal	Network Access to Privileged Commands	IAC-21.6	Mechanisms exist to authorize remote access to perform privileged commands on critical Technology Assets, Applications and/or Services (TAAS) or where sensitive/regulated data is stored, transmitted and/or processed only for compelling operational needs.	10		High
AC-06(04)	Least Privilege | Separate Processing Domains	Provide separate processing domains to enable finer-grained allocation of user privileges.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
AC-06(05)	Least Privilege | Privileged Accounts	Restrict privileged accounts on the system to [Assignment: organization-defined personnel or roles].	Functional	Equal	Management Approval For Privileged Accounts	IAC-21.3	Mechanisms exist to restrict the assignment of privileged accounts to management-approved personnel and/or roles.	10		Moderate
AC-06(06)	Least Privilege | Privileged Access by Non-organizational Users	Prohibit privileged access to the system by non-organizational users.	Functional	Equal	Privileged Access by Non-Organizational Users	IAC-05.2	Mechanisms exist to prohibit privileged access by non-organizational users.	10		Not Selected
AC-06(07)	Least Privilege | Review of User Privileges	a. Review [Assignment: organization-defined frequency] the privileges assigned to [Assignment: organization-defined roles or classes of users] to validate the need for such privileges; andb. Reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs.	Functional	Equal	Periodic Review of Account Privileges	IAC-17	Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary.	10		Moderate
AC-06(08)	Least Privilege | Privilege Levels for Code Execution	Prevent the following software from executing at higher privilege levels than users executing the software: [Assignment: organization-defined software].	Functional	Equal	Privilege Levels for Code Execution	IAC-21.7	Automated mechanisms exist to prevent applications from executing at higher privilege levels than the user's privileges.	10		Not Selected
AC-06(09)	Least Privilege | Log Use of Privileged Functions	Log the execution of privileged functions.	Functional	Equal	Auditing Use of Privileged Functions	IAC-21.4	Mechanisms exist to audit the execution of privileged functions.	10		Moderate
AC-06(10)	Least Privilege | Prohibit Non-privileged Users from Executing Privileged Functions	Prevent non-privileged users from executing privileged functions.	Functional	Equal	Prohibit Non-Privileged Users from Executing Privileged Functions	IAC-21.5	Mechanisms exist to prevent non-privileged users from executing privileged functions to include disabling, circumventing or altering implemented security safeguards / countermeasures.	10		Moderate
AC-07	Unsuccessful Logon Attempts	a. Enforce a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period]; andb. Automatically [Selection (one or more): lock the account or node for an [Assignment: organization-defined time period]; lock the account or node until released by an administrator; delay next logon prompt per [Assignment: organization-defined delay algorithm]; notify system administrator; take other [Assignment: organization-defined action]] when the maximum number of unsuccessful attempts is exceeded.	Functional	Equal	Account Lockout	IAC-22	Mechanisms exist to enforce a limit for consecutive invalid login attempts by a user during an organization-defined time period and automatically locks the account when the maximum number of unsuccessful attempts is exceeded.	10		Low
AC-07(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
AC-07(02)	Unsuccessful Logon Attempts | Purge or Wipe Mobile Device	Purge or wipe information from [Assignment: organization-defined mobile devices] based on [Assignment: organization-defined purging or wiping requirements and techniques] after [Assignment: organization-defined number] consecutive, unsuccessful device logon attempts.	Functional	Equal	Remote Purging	MDM-05	Mechanisms exist to remotely purge selected information from mobile devices.	10		Not Selected
AC-07(03)	Unsuccessful Logon Attempts | Biometric Attempt Limiting	Limit the number of unsuccessful biometric logon attempts to [Assignment: organization-defined number].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
AC-07(04)	Unsuccessful Logon Attempts | Use of Alternate Authentication Factor	a. Allow the use of [Assignment: organization-defined authentication factors] that are different from the primary authentication factors after the number of organization-defined consecutive invalid logon attempts have been exceeded; andb. Enforce a limit of [Assignment: organization-defined number] consecutive invalid logon attempts through use of the alternative factors by a user during a [Assignment: organization-defined time period].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh	Notes	NIST SP 800-53B Baseline
AC-08	System Use Notification	a. Display [Assignment: organization-defined system use notification message or banner] to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and state that:1. Users are accessing a U.S. Government system;2. System usage may be monitored, recorded, and subject to audit;3. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and4. Use of the system indicates consent to monitoring and recording;b. Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system; andc. For publicly accessible systems:1. Display system use information [Assignment: organization-defined conditions], before granting further access to the publicly accessible system;2. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and3. Include a description of the authorized uses of the system.	Functional	Equal	System Use Notification (Logon Banner)	SEA-18	Mechanisms exist to utilize system use notification / logon banners that display an approved system use notification message or banner before granting access to Technology Assets, Applications and/or Services (TAAS).	10		Low
AC-09	Previous Logon Notification	Notify the user, upon successful logon to the system, of the date and time of the last logon.	Functional	Equal	Previous Logon Notification	SEA-19	Mechanisms exist to configure systems that process, store or transmit sensitive/regulated data to notify the user, upon successful logon, of the number of unsuccessful logon attempts since the last successful logon.	10		Not Selected
AC-09(01)	Previous Logon Notification | Unsuccessful Logons	Notify the user, upon successful logon, of the number of unsuccessful logon attempts since the last successful logon.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
AC-09(02)	Previous Logon Notification | Successful and Unsuccessful Logons	Notify the user, upon successful logon, of the number of [Selection (one): successful logons; unsuccessful logon attempts; both] during [Assignment: organization-defined time period].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
AC-09(03)	Previous Logon Notification | Notification of Account Changes	Notify the user, upon successful logon, of changes to [Assignment: organization-defined security-related characteristics or parameters of the user's account] during [Assignment: organization-defined time period].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
AC-09(04)	Previous Logon Notification | Additional Logon Information	Notify the user, upon successful logon, of the following additional information: [Assignment: organization-defined additional information].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
AC-10	Concurrent Session Control	Limit the number of concurrent sessions for each [Assignment: organization-defined account and/or account type] to [Assignment: organization-defined number].	Functional	Equal	Concurrent Session Control	IAC-23	Mechanisms exist to limit the number of concurrent sessions for each system account.	10		High
AC-11	Device Lock	a. Prevent further access to the system by [Selection (one or more): initiating a device lock after [Assignment: organization-defined time period] of inactivity; requiring the user to initiate a device lock before leaving the system unattended]; andb. Retain the device lock until the user reestablishes access using established identification and authentication procedures.	Functional	Intersects With	Session Lock	IAC-24	Mechanisms exist to initiate a session lock after an organization-defined time period of inactivity, or upon receiving a request from a user and retain the session lock until the user reestablishes access using established identification and authentication methods.	5		Moderate
AC-11(01)	Device Lock | Pattern-hiding Displays	Conceal, via the device lock, information previously visible on the display with a publicly viewable image.	Functional	Equal	Pattern-Hiding Displays	IAC-24.1	Mechanisms exist to implement pattern-hiding displays to conceal information previously visible on the display during the session lock.	10		Moderate
AC-12	Session Termination	Automatically terminate a user session after [Assignment: organization-defined conditions or trigger events requiring session disconnect].	Functional	Equal	Session Termination	IAC-25	Automated mechanisms exist to log out users, both locally on the network and for remote sessions, at the end of the session or after an organization-defined period of inactivity.	10		Moderate
AC-12(01)	Session Termination | User-initiated Logouts	Provide a logout capability for user-initiated communications sessions whenever authentication is used to gain access to [Assignment: organization-defined information resources].	Functional	Equal	User-Initiated Logouts / Message Displays	IAC-25.1	Mechanisms exist to provide a logout capability and display an explicit logout message to users indicating the reliable termination of the session.	10		Not Selected
AC-12(02)	Session Termination | Termination Message	Display an explicit logout message to users indicating the termination of authenticated communications sessions.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
AC-12(03)	Session Termination | Timeout Warning Message	Display an explicit message to users indicating that the session will end in [Assignment: organization-defined time until end of session].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
AC-13		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
AC-14	Permitted Actions Without Identification or Authentication	a. Identify [Assignment: organization-defined user actions] that can be performed on the system without identification or authentication consistent with organizational mission and business functions; andb. Document and provide supporting rationale in the security plan for the system, user actions not requiring identification or authentication.	Functional	Equal	Permitted Actions Without Identification or Authorization	IAC-26	Mechanisms exist to identify and document the supporting rationale for specific user actions that can be performed on a system without identification or authentication.	10		Low
AC-14(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
AC-15		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
AC-16	Security and Privacy Attributes	a. Provide the means to associate [Assignment: organization-defined types of security and privacy attributes] with [Assignment: organization-defined security and privacy attribute values] for information in storage, in process, and/or in transmission;b. Ensure that the attribute associations are made and retained with the information;c. Establish the following permitted security and privacy attributes from the attributes defined in AC-16a for [Assignment: organization-defined systems]: [Assignment: organization-defined security and privacy attributes];d. Determine the following permitted attribute values or ranges for each of the established attributes: [Assignment: organization-defined attribute values or ranges for established attributes];e. Audit changes to attributes; andf. Review [Assignment: organization-defined security and privacy attributes] for applicability [Assignment: organization-defined frequency].	Functional	Equal	Cybersecurity & Data Protection Attributes	DCH-05	Mechanisms exist to bind cybersecurity and data protection attributes to information as it is stored, transmitted and processed.	10		Not Selected
AC-16(01)	Security and Privacy Attributes | Dynamic Attribute Association	Dynamically associate security and privacy attributes with [Assignment: organization-defined subjects and objects] in accordance with the following security and privacy policies as information is created and combined: [Assignment: organization-defined security and privacy policies].	Functional	Equal	Dynamic Attribute Association	DCH-05.1	Mechanisms exist to dynamically associate cybersecurity and data protection attributes with individuals and objects as information is created, combined, or transformed, in accordance with organization-defined cybersecurity and data protection policies.	10		Not Selected
AC-16(02)	Security and Privacy Attributes | Attribute Value Changes by Authorized Individuals	Provide authorized individuals (or processes acting on behalf of individuals) the capability to define or change the value of associated security and privacy attributes.	Functional	Equal	Attribute Value Changes By Authorized Individuals	DCH-05.2	Mechanisms exist to provide authorized individuals (or processes acting on behalf of individuals) the capability to define or change the value of associated cybersecurity and data protection attributes.	10		Not Selected
AC-16(03)	Security and Privacy Attributes | Maintenance of Attribute Associations by System	Maintain the association and integrity of [Assignment: organization-defined security and privacy attributes] to [Assignment: organization-defined subjects and objects].	Functional	Equal	Maintenance of Attribute Associations By System	DCH-05.3	Mechanisms exist to maintain the association and integrity of cybersecurity and data protection attributes to individuals and objects.	10		Not Selected
AC-16(04)	Security and Privacy Attributes | Association of Attributes by Authorized Individuals	Provide the capability to associate [Assignment: organization-defined security and privacy attributes] with [Assignment: organization-defined subjects and objects] by authorized individuals (or processes acting on behalf of individuals).	Functional	Equal	Association of Attributes By Authorized Individuals	DCH-05.4	Mechanisms exist to provide the capability to associate cybersecurity and data protection attributes with individuals and objects by authorized individuals (or processes acting on behalf of individuals).	10		Not Selected

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh	Notes	NIST SP 800-53B Baseline
AC-16(05)	Security and Privacy Attributes | Attribute Displays on Objects to Be Output	Display security and privacy attributes in human-readable form on each object that the system transmits to output devices to identify [Assignment: organization-defined special dissemination, handling, or distribution instructions] using [Assignment: organization-defined human-readable, standard naming conventions].	Functional	Equal	Attribute Displays for Output Devices	DCH-05.5	Mechanisms exist to display cybersecurity and data protection attributes in human-readable form on each object that the system transmits to output devices to identify special dissemination, handling or distribution instructions using human-readable, standard naming conventions.	10		Not Selected
AC-16(06)	Security and Privacy Attributes | Maintenance of Attribute Association	Require personnel to associate and maintain the association of [Assignment: organization-defined security and privacy attributes] with [Assignment: organization-defined subjects and objects] in accordance with [Assignment: organization-defined security and privacy policies].	Functional	Equal	Data Subject Attribute Associations	DCH-05.6	Mechanisms exist to require personnel to associate and maintain the association of cybersecurity and data protection attributes with individuals and objects in accordance with cybersecurity and data protection policies.	10		Not Selected
AC-16(07)	Security and Privacy Attributes | Consistent Attribute Interpretation	Provide a consistent interpretation of security and privacy attributes transmitted between distributed system components.	Functional	Equal	Consistent Attribute Interpretation	DCH-05.7	Mechanisms exist to provide a consistent, organizationally agreed upon interpretation of cybersecurity and data protection attributes employed in access enforcement and flow enforcement decisions between distributed system components.	10		Not Selected
AC-16(08)	Security and Privacy Attributes | Association Techniques and Technologies	Implement [Assignment: organization-defined techniques and technologies] in associating security and privacy attributes to information.	Functional	Equal	Identity Association Techniques & Technologies	DCH-05.8	Mechanisms exist to associate cybersecurity and data protection attributes to information.	10		Not Selected
AC-16(09)	Privacy Attributes | Attribute Reassignment — Regrading	Change security and privacy attributes associated with information only via regrading mechanisms validated using [Assignment: organization-defined techniques or procedures].	Functional	Equal	Attribute Reassignment	DCH-05.9	Mechanisms exist to reclassify data as required, due to changing business/technical requirements.	10		Not Selected
AC-16(10)	Security and Privacy Attributes | Attribute Configuration by Authorized Individuals	Provide authorized individuals the capability to define or change the type and value of security and privacy attributes available for association with subjects and objects.	Functional	Equal	Attribute Configuration By Authorized Individuals	DCH-05.10	Mechanisms exist to provide authorized individuals the capability to define or change the type and value of cybersecurity and data protection attributes available for association with subjects and objects.	10		Not Selected
AC-17	Remote Access	a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; andb. Authorize each type of remote access to the system prior to allowing such connections.	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5		Low
AC-17(01)	Remote Access | Monitoring and Control	Employ automated mechanisms to monitor and control remote access methods.	Functional	Equal	Automated Monitoring & Control	NET-14.1	Automated mechanisms exist to monitor and control remote access sessions.	10		Moderate
AC-17(02)	Remote Access | Protection of Confidentiality and Integrity Using Encryption	Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.	Functional	Equal	Protection of Confidentiality / Integrity Using Encryption	NET-14.2	Cryptographic mechanisms exist to protect the confidentiality and integrity of remote access sessions (e.g., VPN).	10		Moderate
AC-17(03)	Remote Access | Managed Access Control Points	Route remote accesses through authorized and managed network access control points.	Functional	Equal	Managed Access Control Points	NET-14.3	Mechanisms exist to route all remote accesses through managed network access control points (e.g., VPN concentrator).	10		Moderate
AC-17(04)	Remote Access | Privileged Commands and Access	a. Authorize the execution of privileged commands and access to security-relevant information via remote access only in a format that provides assessable evidence and for the following needs: [Assignment: organization-defined needs]; andb. Document the rationale for remote access in the security plan for the system.	Functional	Equal	Remote Privileged Commands & Sensitive Data Access	NET-14.4	Mechanisms exist to restrict the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs.	10		Moderate
AC-17(05)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
AC-17(06)	Remote Access | Protection of Mechanism Information	Protect information about remote access mechanisms from unauthorized use and disclosure.	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5		Not Selected
AC-17(07)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
AC-17(08)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
AC-17(09)	Remote Access | Disconnect or Disable Access	Provide the capability to disconnect or disable remote access to the system within [Assignment: organization-defined time period].	Functional	Equal	Expeditious Disconnect / Disable Capability	NET-14.8	Mechanisms exist to provide the capability to expeditiously disconnect or disable a user's remote access session.	10		Not Selected
AC-17(10)	Remote Access | Authenticate Remote Commands	Implement [Assignment: organization-defined mechanisms] to authenticate [Assignment: organization-defined remote commands].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
AC-18	Wireless Access	a. Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access; andb. Authorize each type of wireless access to the system prior to allowing such connections.	Functional	Intersects With	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5		Low
AC-18	Wireless Access	a. Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access; andb. Authorize each type of wireless access to the system prior to allowing such connections.	Functional	Intersects With	Wireless Access Authentication & Encryption	CRY-07	Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption.	5		Low
AC-18(01)	Wireless Access | Authentication and Encryption	Protect wireless access to the system using authentication of [Selection (one or more): users; devices] and encryption.	Functional	Equal	Authentication & Encryption	NET-15.1	Mechanisms exist to secure Wi-Fi (e.g., IEEE 802.11) and prevent unauthorized access by: (1) Authenticating devices trying	10		Moderate
AC-18(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
AC-18(03)	Wireless Access | Disable Wireless Networking	Disable, when not intended for use, wireless networking capabilities embedded within system components prior to issuance and deployment.	Functional	Equal	Disable Wireless Networking	NET-15.2	Mechanisms exist to disable unnecessary wireless networking capabilities that are internally embedded within system components prior to issuance to end users.	10		Moderate
AC-18(04)	Wireless Access | Restrict Configurations by Users	Identify and explicitly authorize users allowed to independently configure wireless networking capabilities.	Functional	Equal	Restrict Configuration By Users	NET-15.3	Mechanisms exist to identify and explicitly authorize users who are allowed to independently configure wireless networking capabilities.	10		High
AC-18(05)	Wireless Access | Antennas and Transmission Power Levels	Select radio antennas and calibrate transmission power levels to reduce the probability that signals from wireless access points can be received outside of organization-controlled boundaries.	Functional	Equal	Wireless Boundaries	NET-15.4	Mechanisms exist to confine wireless communications to organization-controlled boundaries.	10		High
AC-19	Access Control for Mobile Devices	a. Establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas; andb. Authorize the connection of mobile devices to organizational systems.	Functional	Equal	Access Control For Mobile Devices	MDM-02	Mechanisms exist to enforce access control requirements for the connection of mobile devices to organizational Technology Assets, Applications and/or Services (TAAS).	10		Low
AC-19(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
AC-19(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
AC-19(03)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-53B Baseline
AC-19(04)	Access Control for Mobile Devices | Restrictions for Classified Information	a. Prohibit the use of unclassified mobile devices in facilities containing systems processing, storing, or transmitting classified information unless specifically permitted by the authorizing official; andb. Enforce the following restrictions on individuals permitted by the authorizing official to use unclassified mobile devices in facilities containing systems processing, storing, or transmitting classified information:1. Connection of unclassified mobile devices to classified systems is prohibited;2. Connection of unclassified mobile devices to unclassified systems requires approval from the authorizing official;3. Use of internal or external modems or wireless interfaces within the unclassified mobile devices is prohibited; and4. Unclassified mobile devices and the information stored on those devices are subject to random reviews and inspections by [Assignment: organization-defined security officials], and if classified information is found, the incident handling policy is followed.c. Restrict the connection of classified mobile devices to classified systems in accordance with [Assignment: organization-defined security policies].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
AC-19(05)	Access Control for Mobile Devices | Full Device or Container-based Encryption	Employ [Selection: full-device encryption; container-based encryption] to protect the confidentiality and integrity of information on [Assignment: organization-defined mobile devices].	Functional	Equal	Full Device & Container-Based Encryption	MDM-03	Cryptographic mechanisms exist to protect the confidentiality and integrity of information on mobile devices through full-device or container encryption.	10		Moderate
AC-20	Use of External Systems	a. [Selection (one or more): Establish [Assignment: organization-defined terms and conditions]; Identify [Assignment: organization-defined controls asserted to be implemented on external systems]], consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to:1. Access the system from external systems; and2. Process, store, or transmit organization-controlled information using external systems; orb. Prohibit the use of [Assignment: organizationally-defined types of external systems].	Functional	Equal	Use of External Technology Assets, Applications and/or Services (TAAS)	DCH-13	Mechanisms exist to govern how external parties, including Technology Assets, Applications and/or Services (TAAS), are used to securely store, process and transmit data.	10		Low
AC-20(01)	Use of External Systems | Limits on Authorized Use	Permit authorized individuals to use an external system to access the system or to process, store, or transmit organization-controlled information only after:a. Verification of the implementation of controls on the external system as specified in the organization's security and privacy policies and security and privacy plans; orb. Retention of approved system connection or processing agreements with the organizational entity hosting the external system.	Functional	Equal	Limits of Authorized Use	DCH-13.1	Mechanisms exist to prohibit external parties, including Technology Assets, Applications and/or Services (TAAS), from storing, processing and transmitting data unless authorized individuals first: (1) Verifying the implementation of required security, compliance and/or resilience controls; or (2) Retaining a processing agreement with the entity hosting the external TAAS.	10		Moderate
AC-20(02)	Use of External Systems | Portable Storage Devices — Restricted Use	Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems using [Assignment: organization-defined restrictions].	Functional	Intersects With	Portable Storage Devices	DCH-13.2	Mechanisms exist to restrict or prohibit the use of portable storage devices by users on external systems.	5		Moderate
AC-20(03)	Use of External Systems | Non-organizationally Owned Systems — Restricted Use	Restrict the use of non-organizationally owned systems or system components to process, store, or transmit organizational information using [Assignment: organization-defined restrictions].	Functional	Equal	Non-Organizationally Owned Technology Assets, Applications and/or Services (TAAS)	DCH-13.4	Mechanisms exist to restrict the use of non-organizationally owned Technology Assets, Applications and/or Services (TAAS) to process, store or transmit organizational	10		Not Selected
AC-20(04)	Use of External Systems | Network Accessible Storage Devices — Prohibited Use	Prohibit the use of [Assignment: organization-defined network accessible storage devices] in external systems.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
AC-20(05)	Use of External Systems | Portable Storage Devices — Prohibited Use	Prohibit the use of organization-controlled portable storage devices by authorized individuals on external systems.	Functional	Equal	Portable Storage Devices	DCH-13.2	Mechanisms exist to restrict or prohibit the use of portable storage devices by users on external systems.	10		Not Selected
AC-21	Information Sharing	a. Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions for [Assignment: organization-defined information sharing circumstances where user discretion is required]; andb. Employ [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing and collaboration decisions.	Functional	Intersects With	Information Sharing With Third Parties	PRI-07	Mechanisms exist to disclose Personal Data (PD) to third-parties only for the purposes identified in the data privacy notice and with the implicit or explicit consent of the data subject.	5		Moderate
AC-21	Information Sharing	a. Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions for [Assignment: organization-defined information sharing circumstances where user discretion is required]; andb. Employ [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing and collaboration decisions.	Functional	Intersects With	Information Sharing	DCH-14	Mechanisms exist to utilize a process to assist users in making information sharing decisions to ensure data is appropriately protected.	5		Moderate
AC-21(01)	Information Sharing | Automated Decision Support	Employ [Assignment: organization-defined automated mechanisms] to enforce information-sharing decisions by authorized users based on access authorizations of sharing partners and access restrictions on information to be shared.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
AC-21(02)	Information Sharing | Information Search and Retrieval	Implement information search and retrieval services that enforce [Assignment: organization-defined information sharing restrictions].	Functional	Equal	Information Search & Retrieval	DCH-14.1	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) implement data search and retrieval functions that properly enforce data protection / sharing	10		Not Selected
AC-22	Publicly Accessible Content	a. Designate individuals authorized to make information publicly accessible;b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information;c. Review the proposed content of information prior to posting onto the publicly accessible system to ensure that nonpublic information is not included; andd. Review the content on the publicly accessible system for nonpublic information [Assignment: organization-defined frequency] and remove such information, if discovered.	Functional	Equal	Publicly Accessible Content	DCH-15	Mechanisms exist to control publicly-accessible content.	10		Low
AC-23	Data Mining Protection	Employ [Assignment: organization-defined data mining prevention and detection techniques] for [Assignment: organization-defined data storage objects] to detect and protect against unauthorized data mining.	Functional	Intersects With	Data Mining Protection	DCH-16	Mechanisms exist to protect data storage objects against unauthorized data mining and data harvesting techniques.	5		Not Selected
AC-23	Data Mining Protection	Employ [Assignment: organization-defined data mining prevention and detection techniques] for [Assignment: organization-defined data storage objects] to detect and protect against unauthorized data mining.	Functional	Intersects With	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to: (1) The purpose(s) originally	5		Not Selected
AC-24	Access Control Decisions	[Selection (one or more): Establish procedures; Implement mechanisms] to ensure [Assignment: organization-defined access control decisions] are applied to each access request prior to access enforcement.	Functional	Intersects With	Management Approval For New or Changed Accounts	IAC-28.1	Mechanisms exist to ensure management approvals are required for new accounts or changes in permissions to existing accounts.	5		Not Selected
AC-24(01)	Access Control Decisions | Transmit Access Authorization Information	Transmit [Assignment: organization-defined access authorization information] using [Assignment: organization-defined controls] to [Assignment: organization-defined systems] that enforce access control decisions.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
AC-24(02)	Access Control Decisions | No User or Process Identity	Enforce access control decisions based on [Assignment: organization-defined security or privacy attributes] that do not include the identity of the user or process acting on behalf of the user.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
AC-25	Reference Monitor	Implement 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.	Functional	Equal	Reference Monitor	IAC-27	Mechanisms exist to implement a reference monitor that is tamperproof, always-invoked, small enough to be subject to analysis / testing and the completeness of which can be assured.	10		Not Selected

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-53B Baseline
AT-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] awareness and training policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the awareness and training policy and the associated awareness and training controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the awareness and training policy and procedures; andc. Review and update the current awareness and training:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5		Low
AT-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] awareness and training policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the awareness and training policy and the associated awareness and training controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the awareness and training policy and procedures; andc. Review and update the current awareness and training:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10		Low
AT-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] awareness and training policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the awareness and training policy and the associated awareness and training controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the awareness and training policy and procedures; andc. Review and update the current awareness and training:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5		Low
AT-02	Literacy Training and Awareness	a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors):1. As part of initial training for new users and [Assignment: organization-defined frequency] thereafter; and2. When required by system changes or following [Assignment: organization-defined events];b. Employ the following techniques to increase the security and privacy awareness of system users [Assignment: organization-defined awareness techniques];c. Update literacy training and awareness content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; andd. Incorporate lessons learned from internal or external security incidents or breaches into literacy training and awareness techniques.	Functional	Equal	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	10		Low
AT-02(01)	Literacy Training and Awareness | Practical Exercises	Provide practical exercises in literacy training that simulate events and incidents.	Functional	Intersects With	Simulated Cyber Attack Scenario Training	SAT-02.1	Mechanisms exist to include simulated actual cyber-attacks through practical exercises that are aligned with current threat scenarios.	5		Not Selected
AT-02(02)	Literacy Training and Awareness | Insider Threat	Provide literacy training on recognizing and reporting potential indicators of insider threat.	Functional	Equal	Insider Threat Awareness	THR-05	Mechanisms exist to utilize security awareness training on recognizing and reporting potential indicators of insider threat.	10		Low
AT-02(03)	Literacy Training and Awareness | Social Engineering and Mining	Provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining.	Functional	Equal	Social Engineering & Mining	SAT-02.2	Mechanisms exist to include awareness training on recognizing and reporting potential and actual instances of social engineering and social	10		Moderate
AT-02(04)	Literacy Training and Awareness | Suspicious Communications and Anomalous System Behavior	Provide literacy training on recognizing suspicious communications and anomalous behavior in organizational systems using [Assignment: organization-defined indicators of malicious code].	Functional	Intersects With	Suspicious Communications & Anomalous System Behavior	SAT-03.2	Mechanisms exist to provide training to personnel on organization-defined indicators of malware to recognize suspicious communications and anomalous behavior.	5		Not Selected
AT-02(05)	Literacy Training and Awareness | Advanced Persistent Threat	Provide literacy training on the advanced persistent threat.	Functional	Intersects With	Suspicious Communications & Anomalous System Behavior	SAT-03.2	Mechanisms exist to provide training to personnel on organization-defined indicators of malware to recognize suspicious communications and anomalous behavior.	5		Not Selected
AT-02(06)	Literacy Training and Awareness | Cyber Threat Environment	a. Provide literacy training on the cyber threat environment; andb. Reflect current cyber threat information in system operations.	Functional	Equal	Cyber Threat Environment	SAT-03.6	Mechanisms exist to provide role-based security, compliance and resilience awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.	10		Not Selected
AT-03	Role-based Training	a. Provide role-based security and privacy training to personnel with the following roles and responsibilities: [Assignment: organization-defined roles and responsibilities]:1. Before authorizing access to the system, information, or performing assigned duties, and [Assignment: organization-defined frequency] thereafter; and2. When required by system changes;b. Update role-based training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; andc. Incorporate lessons learned from internal or external security incidents or breaches into role-based training.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5		Low
AT-03(01)	Role-based Training | Environmental Controls	Provide [Assignment: organization-defined personnel or roles] with initial and [Assignment: organization-defined frequency] training in the employment and operation of environmental controls.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
AT-03(02)	Role-based Training | Physical Security Controls	Provide [Assignment: organization-defined personnel or roles] with initial and [Assignment: organization-defined frequency] training in the employment and operation of physical security controls.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5		Not Selected
AT-03(03)	Role-based Training | Practical Exercises	Provide practical exercises in security and privacy training that reinforce training objectives.	Functional	Equal	Practical Exercises	SAT-03.1	Mechanisms exist to include practical exercises in security, compliance and resilience training that reinforce training objectives.	10		Not Selected
AT-03(04)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-53B Baseline
AT-03(05)	Role-based Training | Processing Personally Identifiable Information	Provide [Assignment: organization-defined personnel or roles] with initial and [Assignment: organization-defined frequency] training in the employment and operation of personally identifiable information processing and transparency controls.	Functional	Equal	Sensitive / Regulated Data Storage, Handling & Processing	SAT-03.3	Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive/regulated data is formally trained in data handling requirements.	10		Not Selected
AT-04	Training Records	a. Document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training; andb. Retain individual training records for [Assignment: organization-defined time period].	Functional	Equal	Security, Compliance & Resilience Training Records	SAT-04	training activities, including: (1) Initial security, compliance and resilience awareness training; (2) Recurring awareness training; and (3) Technology Assets,	10		Low
AT-05		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
AT-06	Training Feedback	Provide feedback on organizational training results to the following personnel [Assignment: organization-defined frequency]: [Assignment: organization-defined personnel].	Functional	Intersects With	Simulated Cyber Attack Scenario Training	SAT-02.1	Mechanisms exist to include simulated actual cyber-attacks through practical exercises that are aligned with current threat scenarios.	5		Not Selected
AU-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] audit and accountability policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the audit and accountability policy and procedures; andc. Review and update the current audit and accountability:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5		Low
AU-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] audit and accountability policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the audit and accountability policy and procedures; andc. Review and update the current audit and accountability:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5		Low
AU-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] audit and accountability policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the audit and accountability policy and procedures; andc. Review and update the current audit and accountability:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10		Low
AU-02	Event Logging	a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging];b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;c. Specify the following event types for logging within the system: [Assignment: organization-defined event types (subset of the event types defined in AU-02a.) along with the frequency of (or situation requiring) logging for each identified event type];d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; ande. Review and update the event types selected for logging [Assignment: organization-defined frequency]	Functional	Intersects With	Security Event Monitoring	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5		Low
AU-02	Event Logging	a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging];b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;c. Specify the following event types for logging within the system: [Assignment: organization-defined event types (subset of the event types defined in AU-02a.) along with the frequency of (or situation requiring) logging for each identified event type];d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; ande. Review and update the event types selected for logging [Assignment: organization-defined frequency].	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	5		Low
AU-02(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
AU-02(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
AU-02(03)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
AU-02(04)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
AU-03	Content of Audit Records	Ensure that audit records contain information that establishes the following:a. What type of event occurred;b. When the event occurred;c. Where the event occurred;d. Source of the event;e. Outcome of the event; andf. Identity of any individuals, subjects, or objects/entities associated with the event.	Functional	Equal	Content of Event Logs	MON-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	10		Low

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-53B Baseline
AU-03(01)	Content of Audit Records | Additional Audit Information	Generate audit records containing the following additional information: [Assignment: organization-defined additional information].	Functional	Intersects With	Sensitive Event Log Information	MON-03.1	Mechanisms exist to protect sensitive/regulated data contained in log files.	5		Moderate
AU-03(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
AU-03(03)	Content of Audit Records | Limit Personally Identifiable Information Elements	Limit personally identifiable information contained in audit records to the following elements identified in the privacy risk assessment: [Assignment: organization-defined elements].	Functional	Equal	Limit Personal Data (PD) In Audit Records	MON-03.5	Mechanisms exist to limit Personal Data (PD) contained in audit records to the elements identified in the Data Privacy Risk Assessment (DPRA).	10		Not Selected
AU-04	Audit Log Storage Capacity	Allocate audit log storage capacity to accommodate [Assignment: organization-defined audit log retention requirements].	Functional	Equal	Event Log Storage Capacity	MON-04	Mechanisms exist to allocate and proactively manage sufficient event log storage capacity to reduce the likelihood of such capacity being exceeded.	10		Low
AU-04(01)	Audit Log Storage Capacity | Transfer to Alternate Storage	Transfer audit logs [Assignment: organization-defined frequency] to a different system, system component, or media other than the system or system component conducting the logging.	Functional	Intersects With	Event Log Backup on Separate Physical Systems / Components	MON-08.1	Mechanisms exist to back up event logs onto a physically different system or system component than the Security Incident Event Manager (SIEM) or similar automated tool.	5		Not Selected
AU-05	Response to Audit Logging Process Failures	a. Alert [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period] in the event of an audit logging process failure; andb. Take the following additional actions: [Assignment: organization-defined additional actions].	Functional	Equal	Response To Event Log Processing Failures	MON-05	Mechanisms exist to alert appropriate personnel in the event of a log processing failure and take actions to remedy the disruption.	10		Low
AU-05(01)	Response to Audit Logging Process Failures | Storage Capacity Warning	Provide a warning to [Assignment: organization-defined personnel, roles, and/or locations] within [Assignment: organization-defined time period] when allocated audit log storage volume reaches [Assignment: organization-defined percentage] of repository maximum audit log storage capacity.	Functional	Equal	Event Log Storage Capacity Alerting	MON-05.2	Automated mechanisms exist to alert appropriate personnel when the allocated volume reaches an organization-defined percentage of maximum event log storage capacity.	10		High
AU-05(02)	Response to Audit Logging Process Failures | Real-time Alerts	Provide an alert within [Assignment: organization-defined real-time period] to [Assignment: organization-defined personnel, roles, and/or locations] when the following audit failure events occur: [Assignment: organization-defined audit logging failure events requiring real-time alerts].	Functional	Intersects With	Real-Time Alerts of Event Logging Failure	MON-05.1	Mechanisms exist to provide 24x7x365 near real-time alerting capability when an event log processing failure occurs.	5		High
AU-05(03)	Response to Audit Logging Process Failures | Configurable Traffic Volume Thresholds	Enforce configurable network communications traffic volume thresholds reflecting limits on audit log storage capacity and [Selection: reject; delay] network traffic above those thresholds.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
AU-05(04)	Response to Audit Logging Process Failures | Shutdown on Failure	Invoke a [Selection (one): full system shutdown; partial system shutdown; degraded operational mode with limited mission or business functionality available] in the event of [Assignment: organization-defined audit logging failures], unless an alternate audit logging capability exists.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
AU-05(05)	Response to Audit Logging Process Failures | Alternate Audit Logging Capability	Provide an alternate audit logging capability in the event of a failure in primary audit logging capability that implements [Assignment: organization-defined alternate audit logging functionality].	Functional	Equal	Alternate Event Logging Capability	MON-13	Mechanisms exist to provide an alternate event logging capability in the event of a failure in primary audit capability.	10		Not Selected
AU-06	Audit Record Review, Analysis, and Reporting	a. Review and analyze system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity] and the potential impact of the inappropriate or unusual activity;b. Report findings to [Assignment: organization-defined personnel or roles]; andc. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	5		Low
AU-06	Audit Record Review, Analysis, and Reporting	a. Review and analyze system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity] and the potential impact of the inappropriate or unusual activity;b. Report findings to [Assignment: organization-defined personnel or roles]; andc. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.	Functional	Intersects With	Audit Level Adjustments	MON-02.6	Mechanisms exist to adjust the level of audit review, analysis and reporting based on evolving threat information from law enforcement, industry associations or other credible sources of threat intelligence.	5		Low
AU-06(01)	Audit Record Review, Analysis, and Reporting | Automated Process Integration	Integrate audit record review, analysis, and reporting processes using [Assignment: organization-defined automated mechanisms].	Functional	Intersects With	Sensitive Event Log Information	MON-03.1	Mechanisms exist to protect sensitive/regulated data contained in log files.	5		Moderate
AU-06(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
AU-06(03)	Audit Record Review, Analysis, and Reporting | Correlate Audit Record Repositories	Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.	Functional	Intersects With	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.	5		Moderate
AU-06(04)	Audit Record Review, Analysis, and Reporting | Central Review and Analysis	Provide and implement the capability to centrally review and analyze audit records from multiple components within the system.	Functional	Equal	Central Review & Analysis	MON-02.2	Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources.	10		Not Selected
AU-06(05)	Audit Record Review, Analysis, and Reporting | Integrated Analysis of Audit Records	Integrate analysis of audit records with analysis of [Selection (one or more): vulnerability scanning information; performance data; system monitoring information; [Assignment: organization-defined data/information collected from other sources]] to further enhance the ability to identify inappropriate or unusual activity.	Functional	Equal	Integration of Scanning & Other Monitoring Information	MON-02.3	Automated mechanisms exist to integrate the analysis of audit records with analysis of vulnerability scanners, network performance, system monitoring and other sources to further enhance the ability to identify inappropriate or unusual activity.	10		High
AU-06(06)	Audit Record Review, Analysis, and Reporting | Correlation with Physical Monitoring	Correlate information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.	Functional	Equal	Correlation with Physical Monitoring	MON-02.4	Automated mechanisms exist to correlate information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual or malevolent activity.	10		High
AU-06(07)	Audit Record Review, Analysis, and Reporting | Permitted Actions	Specify the permitted actions for each [Selection (one or more): system process; role; user] associated with the review, analysis, and reporting of audit record information.	Functional	Equal	Permitted Actions	MON-02.5	Mechanisms exist to specify the permitted actions for both users and Technology Assets, Applications and/or Services (TAAS) associated with the review, analysis and reporting of audit information.	10		Not Selected
AU-06(08)	Audit Record Review, Analysis, and Reporting | Full Text Analysis of Privileged Commands	Perform a full text analysis of logged privileged commands in a physically distinct component or subsystem of the system, or other system that is dedicated to that analysis.	Functional	Equal	Privileged Functions Logging	MON-03.3	Mechanisms exist to log and review the actions of users and/or services with elevated privileges.	10		Not Selected
AU-06(09)	Audit Record Review, Analysis, and Reporting | Correlation with Information from Nontechnical Sources	Correlate information from nontechnical sources with audit record information to enhance organization-wide situational awareness.	Functional	Intersects With	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.	5		Not Selected
AU-06(10)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
AU-07	Audit Record Reduction and Report Generation	Provide and implement an audit record reduction and report generation capability that:a. Supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of incidents; andb. Does not alter the original content or time ordering of audit records.	Functional	Intersects With	Monitoring Reporting	MON-06	Mechanisms exist to provide an event log report generation capability to aid in detecting and assessing anomalous activities.	5		Moderate
AU-07(01)	Audit Record Reduction and Report Generation | Automatic Processing	Provide and implement the capability to process, sort, and search audit records for events of interest based on the following content: [Assignment: organization-defined fields within audit records].	Functional	Intersects With	Monitoring Reporting	MON-06	Mechanisms exist to provide an event log report generation capability to aid in detecting and assessing anomalous activities.	5		Moderate

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-53B Baseline
AU-07(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
AU-08	Time Stamps	a. Use internal system clocks to generate time stamps for audit records; andb. Record time stamps for audit records that meet [Assignment: organization-defined granularity of time measurement] and that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.	Functional	Intersects With	Clock Synchronization	SEA-20	Mechanisms exist to utilize time-synchronization technology to synchronize all critical system clocks.	5		Low
AU-08	Time Stamps	a. Use internal system clocks to generate time stamps for audit records; andb. Record time stamps for audit records that meet [Assignment: organization-defined granularity of time measurement] and that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.	Functional	Intersects With	Time Stamps	MON-07	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to use an authoritative time source to generate time stamps for event logs.	5		Low
AU-08(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
AU-08(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
AU-09	Protection of Audit Information	a. Protect audit information and audit logging tools from unauthorized access, modification, and deletion; andb. Alert [Assignment: organization-defined personnel or roles] upon detection of unauthorized access, modification, or deletion of audit information.	Functional	Equal	Protection of Event Logs	MON-08	Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion.	10		Low
AU-09(01)	Protection of Audit Information | Hardware Write-once Media	Write audit trails to hardware-enforced, write-once media.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
AU-09(02)	Protection of Audit Information | Store on Separate Physical Systems or Components	Store audit records [Assignment: organization-defined frequency] in a repository that is part of a physically different system or system component than the system or component being audited.	Functional	Intersects With	Event Log Backup on Separate Physical Systems / Components	MON-08.1	Mechanisms exist to back up event logs onto a physically different system or system component than the Security Incident Event Manager (SIEM) or similar automated tool.	5		High
AU-09(03)	Protection of Audit Information | Cryptographic Protection	Implement cryptographic mechanisms to protect the integrity of audit information and audit tools.	Functional	Equal	Cryptographic Protection of Event Log Information	MON-08.3	Cryptographic mechanisms exist to protect the integrity of event logs and audit tools.	10		High
AU-09(04)	Protection of Audit Information | Access by Subset of Privileged Users	Authorize access to management of audit logging functionality to only [Assignment: organization-defined subset of privileged users or roles].	Functional	Equal	Access by Subset of Privileged Users	MON-08.2	Mechanisms exist to restrict access to the management of event logs to privileged users with a specific business need.	10		Moderate
AU-09(05)	Protection of Audit Information | Dual Authorization	Enforce dual authorization for [Selection (one or more): movement; deletion] of [Assignment: organization-defined audit information].	Functional	Equal	Dual Authorization for Event Log Movement	MON-08.4	Automated mechanisms exist to enforce dual authorization for the movement or deletion of event logs.	10		Not Selected
AU-09(06)	Protection of Audit Information | Read-only Access	Authorize read-only access to audit information to [Assignment: organization-defined subset of privileged users or roles].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
AU-09(07)	Protection of Audit Information | Store on Component with Different Operating System	Store audit information on a component running a different operating system than the system or component being audited.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
AU-10	Non-repudiation	Provide irrefutable evidence that an individual (or process acting on behalf of an individual) has performed [Assignment: organization-defined actions to be covered by non-repudiation].	Functional	Equal	Non-Repudiation	MON-09	Mechanisms exist to utilize a non-repudiation capability to protect against an individual falsely denying having performed a particular action.	10		High
AU-10(01)	Non-repudiation | Association of Identities	a. Bind the identity of the information producer with the information to [Assignment: organization-defined strength of binding]; andb. Provide the means for authorized individuals to determine the identity of the producer of the information.	Functional	Intersects With	Identity Binding	MON-09.1	Mechanisms exist to bind the identity of the information producer to the information generated.	5		Not Selected
AU-10(02)	Non-repudiation | Validate Binding of Information Producer Identity	a. Validate the binding of the information producer identity to the information at [Assignment: organization-defined frequency]; andb. Perform [Assignment: organization-defined actions] in the event of a validation error.	Functional	Intersects With	Identity Binding	MON-09.1	Mechanisms exist to bind the identity of the information producer to the information generated.	5		Not Selected
AU-10(03)	Non-repudiation | Chain of Custody	Maintain reviewer or releaser credentials within the established chain of custody for information reviewed or released.	Functional	Intersects With	Chain of Custody & Forensics	IRO-08	Mechanisms exist to perform digital forensics and maintain the integrity of the chain of custody, in accordance with applicable laws, regulations and industry-recognized secure practices.	5		Not Selected
AU-10(04)	Non-repudiation | Validate Binding of Information Reviewer Identity	a. Validate the binding of the information reviewer identity to the information at the transfer or release points prior to release or transfer between [Assignment: organization-defined security domains]; andb. Perform [Assignment: organization-defined actions] in the event of a validation error.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
AU-10(05)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
AU-11	Audit Record Retention	Retain audit records for [Assignment: organization-defined time period consistent with records retention policy] to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements.	Functional	Equal	Event Log Retention	MON-10	Mechanisms exist to retain event logs for a time period consistent with records retention requirements to provide support for after-the-fact investigations of security incidents and to meet statutory, regulatory and contractual retention requirements.	10		Low
AU-11(01)	Audit Record Retention | Long-term Retrieval Capability	Employ [Assignment: organization-defined measures] to ensure that long-term audit records generated by the system can be retrieved.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
AU-12	Audit Record Generation	a. Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2a on [Assignment: organization-defined system components];b. Allow [Assignment: organization-defined personnel or roles] to select the event types that are to be logged by specific components of the system; andc. Generate audit records for the event types defined in AU-2c that include the audit record content defined in AU-3.	Functional	Intersects With	Monitoring Reporting	MON-06	Mechanisms exist to provide an event log report generation capability to aid in detecting and assessing anomalous activities.	5		Low
AU-12(01)	Audit Record Generation | System-wide and Time-correlated Audit Trail	Compile audit records from [Assignment: organization-defined system components] into a system-wide (logical or physical) audit trail that is time-correlated to within [Assignment: organization-defined level of tolerance for the relationship between time stamps of individual records in the audit trail].	Functional	Equal	System-Wide / Time-Correlated Audit Trail	MON-02.7	Automated mechanisms exist to compile audit records into an organization-wide audit trail that is time-correlated.	10		High
AU-12(02)	Audit Record Generation | Standardized Formats	Produce a system-wide (logical or physical) audit trail composed of audit records in a standardized format.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
AU-12(03)	Audit Record Generation | Changes by Authorized Individuals	Provide and implement the capability for [Assignment: organization-defined individuals or roles] to change the logging to be performed on [Assignment: organization-defined system components] based on [Assignment: organization-defined selectable event criteria] within [Assignment: organization-defined time thresholds].	Functional	Equal	Changes by Authorized Individuals	MON-02.8	Mechanisms exist to provide privileged users or roles the capability to change the auditing to be performed on specified system components, based on specific event criteria within specified time thresholds.	10		High
AU-12(04)	Audit Record Generation | Query Parameter Audits of Personally Identifiable Information	Provide and implement the capability for auditing the parameters of user query events for data sets containing personally identifiable information.	Functional	Equal	Query Parameter Audits of Personal Data (PD)	MON-06.1	Mechanisms exist to provide and implement the capability for auditing the parameters of user query events for data sets containing Personal Data (PD).	10		Not Selected
AU-13	Monitoring for Information Disclosure	a. Monitor [Assignment: organization-defined open-source information and/or information sites] [Assignment: organization-defined frequency] for evidence of unauthorized disclosure of organizational information; andb. If an information disclosure is discovered:1. Notify [Assignment: organization-defined personnel or roles]; and2. Take the following additional actions: [Assignment: organization-defined additional actions].	Functional	Equal	Monitoring For Information Disclosure	MON-11	Mechanisms exist to monitor for evidence of unauthorized exfiltration or disclosure of non-public information.	10		Not Selected
AU-13(01)	Monitoring for Information Disclosure | Use of Automated Tools	Monitor open-source information and information sites using [Assignment: organization-defined automated mechanisms].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
AU-13(02)	Monitoring for Information Disclosure | Review of Monitored Sites	Review the list of open-source information sites being monitored [Assignment: organization-defined frequency].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh	Notes	NIST SP 800-53B Baseline
AU-13(03)	Monitoring for Information Disclosure | Unauthorized Replication of Information	Employ discovery techniques, processes, and tools to determine if external entities are replicating organizational information in an unauthorized manner.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
AU-14	Session Audit	a. Provide and implement the capability for [Assignment: organization-defined users or roles] to [Selection (one or more): record; view; hear; log] the content of a user session under [Assignment: organization-defined circumstances]; andb. Develop, integrate, and use session auditing activities in consultation with legal counsel and in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.	Functional	Equal	Session Audit	MON-12	Mechanisms exist to provide session audit capabilities that can: (1) Capture and log all content related to a user session; and (2) Remotely view all content related to an established user session in real time.	10		Not Selected
AU-14(01)	Session Audit | System Start-up	Initiate session audits automatically at system start-up.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
AU-14(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
AU-14(03)	Session Audit | Remote Viewing and Listening	Provide and implement the capability for authorized users to remotely view and hear content related to an established user session in real time.	Functional	Equal	Real-Time Session Monitoring	MON-01.17	Mechanisms exist to enable authorized personnel the ability to remotely view and hear content related to an established user session in real time, in accordance with organizational standards, as well as statutory, regulatory and contractual obligations.	10		Not Selected
AU-15		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
AU-16	Cross-organizational Audit Logging	Employ [Assignment: organization-defined methods] for coordinating [Assignment: organization-defined audit information] among external organizations when audit information is transmitted across organizational boundaries.	Functional	Intersects With	Cross-Organizational Monitoring	MON-14	Mechanisms exist to coordinate sanitized event logs among external organizations to identify anomalous events when event logs are shared across organizational boundaries, without giving away sensitive or critical business data.	5		Not Selected
AU-16(01)	Cross-organizational Audit Logging | Identity Preservation	Preserve the identity of individuals in cross-organizational audit trails.	Functional	Intersects With	Cross-Organizational Monitoring	MON-14	Mechanisms exist to coordinate sanitized event logs among external organizations to identify anomalous events when event logs are shared across organizational boundaries, without giving away sensitive or critical business data.	5		Not Selected
AU-16(02)	Cross-organizational Audit Logging | Sharing of Audit Information	Provide cross-organizational audit information to [Assignment: organization-defined organizations] based on [Assignment: organization-defined cross-organizational sharing agreements].	Functional	Equal	Sharing of Event Logs	MON-14.1	Mechanisms exist to share event logs with third-party organizations based on specific cross-organizational sharing agreements.	10		Not Selected
AU-16(03)	Cross-organizational Audit Logging | Disassociability	Implement [Assignment: organization-defined measures] to disassociate individuals from audit information transmitted across organizational boundaries.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
CA-01	Policy and Procedures	[Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] assessment, authorization, and monitoring policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the assessment, authorization, and monitoring policy and the associated assessment, authorization, and monitoring controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the assessment, authorization, and monitoring policy and procedures; andc. Review and update the current assessment, authorization, and monitoring:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10		Low
CA-01	Policy and Procedures	[Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] assessment, authorization, and monitoring policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the assessment, authorization, and monitoring policy and the associated assessment, authorization, and monitoring controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the assessment, authorization, and monitoring policy and procedures; andc. Review and update the current assessment, authorization, and monitoring:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5		Low
CA-01	Policy and Procedures	[Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] assessment, authorization, and monitoring policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the assessment, authorization, and monitoring policy and the associated assessment, authorization, and monitoring controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the assessment, authorization, and monitoring policy and procedures; andc. Review and update the current assessment, authorization, and monitoring:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5		Low
CA-02	Control Assessments	a. Select the appropriate assessor or assessment team for the type of assessment to be conducted;b. Develop a control assessment plan that describes the scope of the assessment including:1. Controls and control enhancements under assessment;2. Assessment procedures to be used to determine control effectiveness; and3. Assessment environment, assessment team, and assessment roles and responsibilities;c. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment;d. Assess the controls in the system and its environment of operation [Assignment: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements;e. Produce a control assessment report that document the results of the assessment; andf. Provide the results of the control assessment to [Assignment: organization-defined individuals or roles].	Functional	Intersects With	Functional Review Of Security, Compliance & Resilience Controls	CPL-03.2	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's security, compliance and/or resilience policies and standards.	5		Low

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-53B Baseline
CA-02	Control Assessments	a. Select the appropriate assessor or assessment team for the type of assessment to be conducted;b. Develop a control assessment plan that describes the scope of the assessment including:1. Controls and control enhancements under assessment;2. Assessment procedures to be used to determine control effectiveness; and3. Assessment environment, assessment team, and assessment roles and responsibilities;c. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment;d. Assess the controls in the system and its environment of operation [Assignment: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements;e. Produce a control assessment report that document the results of the assessment; andf. Provide the results of the control assessment to [Assignment: organization-defined individuals or roles].	Functional	Intersects With	Technical Verification	IAO-06	Mechanisms exist to perform Information Assurance Program (IAP) activities to evaluate the design, implementation and effectiveness of technical security, compliance and resilience controls.	5		Low
CA-02	Control Assessments	a. Select the appropriate assessor or assessment team for the type of assessment to be conducted;b. Develop a control assessment plan that describes the scope of the assessment including:1. Controls and control enhancements under assessment;2. Assessment procedures to be used to determine control effectiveness; and3. Assessment environment, assessment team, and assessment roles and responsibilities;c. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment;d. Assess the controls in the system and its environment of operation [Assignment: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements;e. Produce a control assessment report that document the results of the assessment; andf. Provide the results of the control assessment to [Assignment: organization-defined individuals or roles].	Functional	Intersects With	Security, Compliance & Resilience In Project Management	PRM-04	Mechanisms exist to assess security, compliance and resilience controls in system project development to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the requirements.	5		Low
CA-02	Control Assessments	a. Select the appropriate assessor or assessment team for the type of assessment to be conducted;b. Develop a control assessment plan that describes the scope of the assessment including:1. Controls and control enhancements under assessment;2. Assessment procedures to be used to determine control effectiveness; and3. Assessment environment, assessment team, and assessment roles and responsibilities;c. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment;d. Assess the controls in the system and its environment of operation [Assignment: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements;e. Produce a control assessment report that document the results of the assessment; andf. Provide the results of the control assessment to [Assignment: organization-defined individuals or roles].	Functional	Intersects With	Assessments	IAO-02	Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	5		Low
CA-02	Control Assessments	a. Select the appropriate assessor or assessment team for the type of assessment to be conducted;b. Develop a control assessment plan that describes the scope of the assessment including:1. Controls and control enhancements under assessment;2. Assessment procedures to be used to determine control effectiveness; and3. Assessment environment, assessment team, and assessment roles and responsibilities;c. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment;d. Assess the controls in the system and its environment of operation [Assignment: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements;e. Produce a control assessment report that document the results of the assessment; andf. Provide the results of the control assessment to [Assignment: organization-defined individuals or roles].	Functional	Intersects With	Security, Compliance & Resilience Assessments	CPL-03	Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	5		Low
CA-02(01)	Control Assessments | Independent Assessors	Employ independent assessors or assessment teams to conduct control assessments.	Functional	Equal	Assessor Independence	IAO-02.1	Mechanisms exist to ensure assessors or assessment teams have the appropriate independence to conduct security, compliance and/or resilience control assessments.	10		Moderate
CA-02(02)	Control Assessments | Specialized Assessments	Include as part of control assessments, [Assignment: organization-defined frequency], [Selection (one): announced; unannounced], [Selection (one or more): in-depth monitoring; security instrumentation; automated security test cases; vulnerability scanning; malicious user testing; insider threat assessment; performance and load testing; data leakage or data loss assessment; [Assignment: organization-defined other forms of assessment]].	Functional	Intersects With	Specialized Assessments	IAO-02.2	Mechanisms exist to conduct specialized assessments for: (1) Statutory, regulatory and contractual compliance obligations; (2) Monitoring capabilities; (3) Mobile devices; (4) Databases; (5) Application security; (6) Embedded technologies (e.g., IoT, OT, etc.); (7) Vulnerability management; (8) Malicious code; (9) Insider threats; (10) Performance/load testing; and/or (11) Artificial Intelligence and Autonomous Technologies (AAT).	5		High
CA-02(03)	Control Assessments | Leveraging Results from External Organizations	Leverage the results of control assessments performed by [Assignment: organization-defined external organization(s)] on [Assignment: organization-defined system] when the assessment meets [Assignment: organization-defined requirements].	Functional	Equal	Third-Party Assessment Reciprocity	IAO-02.3	Mechanisms exist to accept and respond to the results of external assessments that are performed by impartial, external organizations.	10		Not Selected
CA-03	Information Exchange	a. Approve and manage the exchange of information between the system and other systems using [Selection (one or more): interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service level agreements; user agreements; nondisclosure agreements; [Assignment: organization-defined type of agreement]];b. Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated; andc. Review and update the agreements [Assignment: organization-defined frequency].	Functional	Intersects With	Interconnection Security Agreements (ISAs)	NET-05	Mechanisms exist to authorize connections from systems to other systems using Interconnection Security Agreements (ISAs), or similar methods, that document, for each interconnection: (1) Interface characteristics; (2) Security, compliance and resilience requirements; and; (3) The nature of the information communicated.	5		Low
CA-03(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
CA-03(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
CA-03(03)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
CA-03(04)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
CA-03(05)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-53B Baseline
CA-03(06)	Information Exchange | Transfer Authorizations	Verify that individuals or systems transferring data between interconnecting systems have the requisite authorizations (i.e., write permissions or privileges) prior to accepting such data.	Functional	Equal	Transfer Authorizations	DCH-14.2	Mechanisms exist to verify that individuals or Technology Assets, Applications and/or Services (TAAS) transferring data between interconnecting TAAS have the requisite authorizations (e.g., write permissions or privileges) prior to transferring said data.	10		High
CA-03(07)	Information Exchange | Transitive Information Exchanges	a. Identify transitive (downstream) information exchanges with other systems through the systems identified in CA-3a; andb. Take measures to ensure that transitive (downstream) information exchanges cease when the controls on identified transitive (downstream) systems cannot be verified or validated.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
CA-04		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
CA-05	Plan of Action and Milestones	a. Develop a plan of action and milestones for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; andb. Update existing plan of action and milestones [Assignment: organization-defined frequency] based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities.	Functional	Intersects With	Capabilities Deficiency Tracking	IAO-05	control; (3) Description of the deficiency(ies); (4) Risk associated with the deficiency(ies); (5) Source deficiency identification/detection; (6) Temporary compensating controls, if applicable; (7) Point of Contact (POC) (e.g	5		Low
CA-05(01)	Plan of Action and Milestones | Automation Support for Accuracy and Currency	Ensure the accuracy, currency, and availability of the plan of action and milestones for the system using [Assignment: organization-defined automated mechanisms].	Functional	Equal	Deficiency Tracking Automation	IAO-05.1	Automated mechanisms exist to help ensure tracked deficiencies are: (1) Accurate; (2) Up-to-date; and (3) Readily-available.	10		Not Selected
CA-06	Authorization	a. Assign a senior official as the authorizing official for the system;b. Assign a senior official as the authorizing official for common controls available for inheritance by organizational systems;c. Ensure that the authorizing official for the system, before commencing operations:1. Accepts the use of common controls inherited by the system; and2. Authorizes the system to operate;d. Ensure that the authorizing official for common controls authorizes the use of those controls for inheritance by organizational systems;e. Update the authorizations [Assignment: organization-defined frequency].	Functional	Equal	Security Authorization	IAO-07	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.	10		Low
CA-06(01)	Authorization | Joint Authorization — Intra-organization	Employ a joint authorization process for the system that includes multiple authorizing officials from the same organization conducting the authorization.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
CA-06(02)	Authorization | Joint Authorization — Inter-organization	Employ a joint authorization process for the system that includes multiple authorizing officials with at least one authorizing official from an organization external to the organization conducting the authorization.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
CA-07	Continuous Monitoring	Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes:a. Establishing the following system-level metrics to be monitored: [Assignment: organization-defined system-level metrics];b. Establishing [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessment of control effectiveness;c. Ongoing control assessments in accordance with the continuous monitoring strategy;d. Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy;e. Correlation and analysis of information generated by control assessments and monitoring;f. Response actions to address results of the analysis of control assessment and monitoring information; andg. Reporting the security and privacy status of the system to [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency].	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5		Low
CA-07(01)	Continuous Monitoring | Independent Assessment	Employ independent assessors or assessment teams to monitor the controls in the system on an ongoing basis.	Functional	Intersects With	Independent Assessors	CPL-03.1	Mechanisms exist to utilize independent assessors to evaluate security, compliance and resilience at planned intervals or when the Technology Asset, Application and/or Service (TAAS) undergoes significant changes.	5		Moderate
CA-07(01)	Continuous Monitoring | Types of Assessments	Employ independent assessors or assessment teams to monitor the controls in the system on an ongoing basis.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5		Moderate
CA-07(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
CA-07(03)	Continuous Monitoring | Trend Analyses	Employ trend analyses to determine if control implementations, the frequency of continuous monitoring activities, and the types of activities used in the continuous monitoring process need to be modified based on empirical data.	Functional	Equal	Trend Analysis Reporting	MON-06.2	Mechanisms exist to employ trend analyses to determine if security control implementations, the frequency of continuous monitoring activities, and/or the types of activities used in the continuous monitoring process need to be modified based on empirical data.	10		Not Selected
CA-07(04)	Continuous Monitoring | Risk Monitoring	Ensure risk monitoring is an integral part of the continuous monitoring strategy that includes the following:a. Effectiveness monitoring;b. Compliance monitoring; andc. Change monitoring.	Functional	Equal	Risk Monitoring	RSK-11	Mechanisms exist to ensure risk monitoring as an integral part of the continuous monitoring strategy that includes monitoring the effectiveness of security, compliance and resilience controls, compliance and change management.	10		Low
CA-07(05)	Continuous Monitoring | Consistency Analysis	Employ the following actions to validate that policies are established and implemented controls are operating in a consistent manner: [Assignment: organization-defined actions].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
CA-07(06)	Continuous Monitoring | Automation Support for Monitoring	Ensure the accuracy, currency, and availability of monitoring results for the system using [Assignment: organization-defined automated mechanisms].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
CA-08	Penetration Testing	Conduct penetration testing [Assignment: organization-defined frequency] on [Assignment: organization-defined systems or system components].	Functional	Equal	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	10		High
CA-08(01)	Penetration Testing | Independent Penetration Testing Agent or Team	Employ an independent penetration testing agent or team to perform penetration testing on the system or system components.	Functional	Equal	Independent Penetration Agent or Team	VPM-07.1	Mechanisms exist to utilize an independent assessor or penetration team to perform penetration testing.	10		High
CA-08(02)	Penetration Testing | Red Team Exercises	Employ the following red-team exercises to simulate attempts by adversaries to compromise organizational systems in accordance with applicable rules of engagement: [Assignment: organization-defined red team exercises].	Functional	Equal	Red Team Exercises	VPM-10	Mechanisms exist to utilize "red team" exercises to simulate attempts by adversaries to compromise Technology Assets, Applications and/or Services (TAAS) in accordance with organization-defined rules of	10		Not Selected
CA-08(03)	Penetration Testing | Facility Penetration Testing	Employ a penetration testing process that includes [Assignment: organization-defined frequency] [Selection (one or more): announced; unannounced] attempts to bypass or circumvent controls associated with physical access points to the facility.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
CA-09	Internal System Connections	a. Authorize internal connections of [Assignment: organization-defined system components or classes of components] to the system;b. Document, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated;c. Terminate internal system connections after [Assignment: organization-defined conditions]; andd. Review [Assignment: organization-defined frequency] the continued need for each internal connection.	Functional	Equal	Internal System Connections	NET-05.2	Mechanisms exist to control internal system connections through authorizing internal connections of systems and documenting, for each internal connection, the interface characteristics, security requirements and the nature of the information communicated.	10		Low

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-53B Baseline
CA-09(01)	Internal System Connections | Compliance Checks	Perform security and privacy compliance checks on constituent system components prior to the establishment of the internal connection.	Functional	Equal	Endpoint Security Validation	NET-14.7	Automated mechanisms exist to validate the security posture of the endpoint devices (e.g., software versions, patch levels, etc.) prior to allowing devices to connect to organizational Technology Assets, Applications and/or Services (TAAS).	10		Not Selected
CM-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] configuration management policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the configuration management policy and the associated configuration management controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the configuration management policy and procedures; andc. Review and update the current configuration management:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Subset Of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10		Low
CM-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] configuration management policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the configuration management policy and the associated configuration management controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the configuration management policy and procedures; andc. Review and update the current configuration management:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5		Low
CM-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] configuration management policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the configuration management policy and the associated configuration management controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the configuration management policy and procedures; andc. Review and update the current configuration management:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5		Low
CM-02	Baseline Configuration	a. Develop, document, and maintain under configuration control, a current baseline configuration of the system; andb. Review and update the baseline configuration of the system:1. [Assignment: organization-defined frequency];2. When required due to [Assignment: organization-defined circumstances]; and3. When system components are installed or	Functional	Intersects With	Reviews & Updates	CFG-02.1	Mechanisms exist to review and update baseline configurations: (1) At least annually; (2) When required due to so; or (3) As part of system component installations and upgrades.	5		Low
CM-02	Baseline Configuration	a. Develop, document, and maintain under configuration control, a current baseline configuration of the system; andb. Review and update the baseline configuration of the system:1. [Assignment: organization-defined frequency];2. When required due to [Assignment: organization-defined circumstances]; and3. When system components are installed or upgraded.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening	5		Low
CM-02(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
CM-02(02)	Baseline Configuration | Automation Support for Accuracy and Currency	Maintain the currency, completeness, accuracy, and availability of the baseline configuration of the system using [Assignment: organization-defined automated mechanisms].	Functional	Equal	Automated Central Management & Verification	CFG-02.2	Automated mechanisms exist to govern and report on baseline configurations of Technology Assets, Applications and/or Services (TAAS) through Continuous Diagnostics and Mitigation (CDM), or similar	10		Moderate
CM-02(03)	Baseline Configuration | Retention of Previous	Retain [Assignment: organization-defined number] of previous versions of baseline configurations of the system to support rollback.	Functional	Equal	Retention Of Previous Configurations	CFG-02.3	Mechanisms exist to retain previous versions of baseline configuration to support roll back.	10		Moderate
CM-02(04)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
CM-02(05)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
CM-02(06)	Baseline Configuration | Development and Test Environments	Maintain a baseline configuration for system development and test environments that is managed separately from the operational baseline configuration.	Functional	Equal	Development & Test Environment Configurations	CFG-02.4	Mechanisms exist to manage baseline configurations for development and test environments separately from operational baseline configurations to minimize the risk of unintentional changes.	10		Not Selected
CM-02(07)	Baseline Configuration | Configure Systems and Components for High-risk Areas	a. Issue [Assignment: organization-defined systems or system components] with [Assignment: organization-defined configurations] to individuals traveling to locations that the organization deems to be of significant risk; andb. Apply the following controls to the systems or components when the individuals return from travel: [Assignment: organization-defined controls].	Functional	Equal	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.	10		Moderate
CM-03	Configuration Change Control	a. Determine and document the types of changes to the system that are configuration-controlled;b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses;c. Document configuration change decisions associated with the system;d. Implement approved configuration-controlled changes to the system;e. Retain records of configuration-controlled changes to the system for [Assignment: organization-defined time period];f. Monitor and review activities associated with configuration-controlled changes to the system; andg. Coordinate and provide oversight for configuration change control activities through [Assignment: organization-defined configuration change control element] that convenes [Selection (one or more): [Assignment: organization-defined frequency]; when [Assignment: organization-defined configuration change conditions]].	Functional	Subset Of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10		Moderate

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-53B Baseline
CM-03	Configuration Change Control	a. Determine and document the types of changes to the system that are configuration-controlled;b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses;c. Document configuration change decisions associated with the system;d. Implement approved configuration-controlled changes to the system;e. Retain records of configuration-controlled changes to the system for [Assignment: organization-defined time period];f. Monitor and review activities associated with configuration-controlled changes to the system; andg. Coordinate and provide oversight for configuration change control activities through [Assignment: organization-defined configuration change control element] that convenes [Selection (one or more): [Assignment: organization-defined frequency]; when [Assignment: organization-defined configuration change conditions]].	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5		Moderate
CM-03(01)	Configuration Change Control | Automated Documentation, Notification, and Prohibition of Changes	Use [Assignment: organization-defined automated mechanisms] to:a. Document proposed changes to the system;b. Notify [Assignment: organization-defined approval authorities] of proposed changes to the system and request change approval;c. Highlight proposed changes to the system that have not been approved or disapproved within [Assignment: organization-defined time period];d. Prohibit changes to the system until designated approvals are received;e. Document all changes to the system; andf. Notify [Assignment: organization-defined personnel] when approved changes to the system are completed.	Functional	Equal	Prohibition Of Changes	CHG-02.1	Mechanisms exist to prohibit unauthorized changes, unless organization-approved change requests are received.	10		High
CM-03(02)	Configuration Change Control | Testing, Validation, and Documentation of Changes	Test, validate, and document changes to the system before finalizing the implementation of the changes.	Functional	Intersects With	Control Functionality Verification	CHG-06	Mechanisms exist to verify the functionality of security, compliance and resilience controls following implemented changes to ensure applicable controls operate as designed.	5		Moderate
CM-03(02)	Configuration Change Control | Testing, Validation, and Documentation of Changes	Test, validate, and document changes to the system before finalizing the implementation of the changes.	Functional	Intersects With	Test, Validate & Document Changes	CHG-02.2	Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented in a production environment.	5		Moderate
CM-03(03)	Configuration Change Control | Automated Change Implementation	Implement changes to the current system baseline and deploy the updated baseline across the installed base using [Assignment: organization-defined automated mechanisms].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
CM-03(04)	Configuration Change Control | Security and Privacy Representatives	Require [Assignment: organization-defined security and privacy representatives] to be members of the [Assignment: organization-defined configuration change control element].	Functional	Equal	Security, Compliance & Resilience Representative for Asset Lifecycle Changes	CHG-02.3	Mechanisms exist to include a cybersecurity and/or data protection representative in the configuration change control review process.	10		Moderate
CM-03(05)	Configuration Change Control | Automated Security Response	Implement the following security responses automatically if baseline configurations are changed in an unauthorized manner: [Assignment: organization-defined security responses].	Functional	Equal	Automated Security Response	CHG-02.4	Automated mechanisms exist to implement remediation actions upon the detection of unauthorized baseline configurations change(s).	10		Not Selected
CM-03(06)	Configuration Change Control | Cryptography Management	Ensure that cryptographic mechanisms used to provide the following controls are under configuration management: [Assignment: organization-defined controls].	Functional	Equal	Cryptographic Management	CHG-02.5	Mechanisms exist to govern assets involved in providing cryptographic protections according to the organization's configuration management processes.	10		High
CM-03(07)	Configuration Change Control | Review System Changes	Review changes to the system [Assignment: organization-defined frequency] or when [Assignment: organization-defined circumstances] to determine whether unauthorized changes have occurred.	Functional	Intersects With	Test, Validate & Document Changes	CHG-02.2	Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented in a production environment.	5		Not Selected
CM-03(08)	Configuration Change Control | Prevent or Restrict Configuration Changes	Prevent or restrict changes to the configuration of the system under the following circumstances: [Assignment: organization-defined circumstances].	Functional	Equal	Configuration Enforcement	CFG-06	Automated mechanisms exist to monitor, enforce and report on configurations for endpoint devices.	10		Not Selected
CM-03(08)	Configuration Change Control | Prevent or Restrict Configuration Changes	Prevent or restrict changes to the configuration of the system under the following circumstances: [Assignment: organization-defined circumstances].	Functional	Intersects With	Integrity Assurance & Enforcement (IAE)	CFG-06.1	Automated mechanisms exist to identify unauthorized deviations from an approved baseline and implement automated resiliency actions to remediate the unauthorized change.	5		Not Selected
CM-04	Impact Analyses	Analyze changes to the system to determine potential security and privacy impacts prior to change implementation.	Functional	Equal	Security Impact Analysis for Changes	CHG-03	Mechanisms exist to analyze proposed changes for potential security impacts, prior to the implementation of the change.	10		Low
CM-04(01)	Impact Analyses | Separate Test Environments	Analyze changes to the system in a separate test environment before implementation in an operational environment, looking for security and privacy impacts due to flaws, weaknesses, incompatibility, or intentional malice.	Functional	Equal	Separation of Development, Testing and Operational Environments	TDA-08	Mechanisms exist to manage separate development, testing and operational environments to reduce the risks of unauthorized access or changes to the operational environment and to ensure no impact to production Technology Assets, Applications and/or Services (TAAS).	10		High
CM-04(02)	Impact Analyses | Verification of Controls	After system changes, verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security and privacy requirements for the system.	Functional	Equal	Technical Verification	IAO-06	Mechanisms exist to perform Information Assurance Program (IAP) activities to evaluate the design, implementation and effectiveness of technical security, compliance and resilience controls.	10		Moderate
CM-05	Access Restrictions for Change	Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.	Functional	Intersects With	Governing Access Restriction for Change	END-03.2	Mechanisms exist to define, document, approve and enforce access restrictions associated with changes to Technology Assets, Applications and/or Services (TAAS).	5		Low
CM-05	Access Restrictions for Change	Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.	Functional	Intersects With	Access Restriction For Change	CHG-04	Mechanisms exist to enforce configuration restrictions in an effort to restrict the ability of users to conduct unauthorized changes.	5		Low
CM-05(01)	Access Restrictions for Change | Automated Access Enforcement and Audit Records	a. Enforce access restrictions using [Assignment: organization-defined automated mechanisms]; andb. Automatically generate audit records of the enforcement actions.	Functional	Equal	Automated Access Enforcement / Auditing	CHG-04.1	Mechanisms exist to perform after-the-fact reviews of configuration change logs to discover any unauthorized changes.	10		High
CM-05(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
CM-05(03)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
CM-05(04)	Access Restrictions for Change | Dual Authorization	Enforce dual authorization for implementing changes to [Assignment: organization-defined system components and system-level information].	Functional	Equal	Dual Authorization for Change	CHG-04.3	Mechanisms exist to enforce a two-person rule for implementing changes to critical Technology Assets, Applications and/or Services (TAAS).	10		Not Selected
CM-05(05)	Access Restrictions for Change | Privilege Limitation for Production and Operation	a. Limit privileges to change system components and system-related information within a production or operational environment; andb. Review and reevaluate privileges [Assignment: organization-defined frequency].	Functional	Equal	Permissions To Implement Changes	CHG-04.4	Mechanisms exist to limit operational privileges for implementing changes.	10		Not Selected
CM-05(06)	Access Restrictions for Change | Limit Library Privileges	Limit privileges to change software resident within software libraries.	Functional	Equal	Library Privileges	CHG-04.5	Mechanisms exist to restrict software library privileges to those individuals with a pertinent business need for access.	10		Not Selected
CM-05(07)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh	Notes	NIST SP 800-53B Baseline
CM-06	Configuration Settings	components employed within the system that reflect the most restrictive mode consistent with operational requirements using [Assignment: organization-defined common secure configurations];b. Implement the configuration settings;c. Identify, document, and approve any deviations from established configuration settings for [Assignment: organization-defined system components] based on [Assignment: organization-defined operational requirements]; andd. Monitor and control changes to the configuration settings in accordance with organizational policies and	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5		Low
CM-06	Configuration Settings	components employed within the system that reflect the most restrictive mode consistent with operational requirements using [Assignment: organization-defined common secure configurations];b. Implement the configuration settings;c. Identify, document, and approve any deviations from established configuration settings for [Assignment: organization-defined system components] based on [Assignment: organization-defined operational requirements]; andd. Monitor and control changes to the configuration settings in accordance with organizational policies and	Functional	Intersects With	Approved Configuration Deviations	CFG-02.7	Mechanisms exist to document, assess risk and approve or deny deviations to standardized configurations.	5		Low
CM-06(01)	Configuration Settings | Automated Management, Application, and Verification	Manage, apply, and verify configuration settings for [Assignment: organization-defined system components] using [Assignment: organization-defined automated mechanisms].	Functional	Intersects With	Automated Central Management & Verification	CFG-02.2	Automated mechanisms exist to govern and report on baseline configurations of Technology Assets, Applications and/or Services (TAAS) through Continuous Diagnostics and Mitigation (CDM), or similar	5		High
CM-06(02)	Configuration Settings | Respond to Unauthorized Changes	Take the following actions in response to unauthorized changes to [Assignment: organization-defined configuration settings]: [Assignment: organization-defined actions].	Functional	Equal	Respond To Unauthorized Changes	CFG-02.8	Mechanisms exist to respond to unauthorized changes to configuration settings as security incidents.	10		High
CM-06(03)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
CM-06(04)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
CM-07	Least Functionality	a. Configure the system to provide only [Assignment: organization-defined mission essential capabilities]; andb. Prohibit or restrict the use of the following functions, ports, protocols, software, and/or services: [Assignment: organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services].	Functional	Equal	Least Functionality	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	10		Low
CM-07(01)	Least Functionality | Periodic Review	a. Review the system [Assignment: organization-defined frequency] to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services; andb. Disable or remove [Assignment: organization-defined functions, ports, protocols, software, and services within the system deemed to be unnecessary and/or nonsecure].	Functional	Equal	Periodic Review	CFG-03.1	Mechanisms exist to periodically review system configurations to identify and disable unnecessary and/or non-secure functions, ports, protocols and services.	10		Moderate
CM-07(02)	Least Functionality | Prevent Program Execution	Prevent program execution in accordance with [Selection (one or more): [Assignment: organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions]; rules authorizing the terms and conditions of software program usage].	Functional	Intersects With	Prevent Program Execution	SEA-06	Automated mechanisms exist to prevent the execution of unauthorized software programs.	5		Moderate
CM-07(02)	Least Functionality | Prevent Program Execution	Prevent program execution in accordance with [Selection (one or more): [Assignment: organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions]; rules authorizing the terms and conditions of software program usage].	Functional	Intersects With	Prevent Unauthorized Software Execution	CFG-03.2	Mechanisms exist to configure systems to prevent the execution of unauthorized software programs.	5		Moderate
CM-07(03)	Least Functionality | Registration Compliance	Ensure compliance with [Assignment: organization-defined registration requirements for functions, ports, protocols, and services].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
CM-07(04)	Least Functionality | Unauthorized Software — Deny-by-exception	a. Identify [Assignment: organization-defined software programs not authorized to execute on the system];b. Employ an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the system; andc. Review and update the list of unauthorized software programs [Assignment: organization-defined frequency].	Functional	Equal	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	10		Not Selected
CM-07(05)	Least Functionality | Authorized Software — Allow-by-exception	a. Identify [Assignment: organization-defined software programs authorized to execute on the system];b. Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system; andc. Review and update the list of authorized software programs [Assignment: organization-defined frequency].	Functional	Equal	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	10		Moderate
CM-07(06)	Least Functionality | Confined Environments with Limited Privileges	Require that the following user-installed software execute in a confined physical or virtual machine environment with limited privileges: [Assignment: organization-defined user-installed software].	Functional	Intersects With	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.	5		Not Selected
CM-07(07)	Least Functionality | Code Execution in Protected Environments	allow execution of binary or machine-executable code only in confined physical or virtual machine environments and with the explicit approval of [Assignment: organization-defined personnel or roles] when such code is:a. Obtained from sources with limited or no warranty; and/orb. Without the provision of source code.	Functional	Intersects With	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.	5		Not Selected
CM-07(08)	Least Functionality | Binary or Machine Executable Code	a. Prohibit the use of binary or machine-executable code from sources with limited or no warranty or without the provision of source code; andb. Allow exceptions only for compelling mission or operational requirements and with the approval of the authorizing official.	Functional	Equal	Binary or Machine-Executable Code	END-06.7	Mechanisms exist to prohibit the use of binary or machine-executable code from sources with limited or no warranty and without access to source code.	10		Not Selected
CM-07(09)	Least Functionality | Prohibiting The Use of Unauthorized Hardware	a. Identify [Assignment: organization-defined hardware components authorized for system use];b. Prohibit the use or connection of unauthorized hardware components;c. Review and update the list of authorized hardware components [Assignment: organization-defined frequency].	Functional	Intersects With	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.	5		Not Selected
CM-08	System Component Inventory	a. Develop and document an inventory of system components that:1. Accurately reflects the system;2. Includes all components within the system;3. Does not include duplicate accounting of components or components assigned to any other system;4. Is at the level of granularity deemed necessary for tracking and reporting; and5. Includes the following information to achieve system component accountability: [Assignment: organization-defined information deemed necessary to achieve effective system component accountability]; andb. Review and update the system component inventory [Assignment: organization-defined frequency].	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	5		Low
CM-08	System Component Inventory	a. Develop and document an inventory of system components that:1. Accurately reflects the system;2. Includes all components within the system;3. Does not include duplicate accounting of components or components assigned to any other system;4. Is at the level of granularity deemed necessary for tracking and reporting; and5. Includes the following information to achieve system component accountability: [Assignment: organization-defined information deemed necessary to achieve effective system component accountability]; andb. Review and update the system component inventory [Assignment: organization-defined frequency].	Functional	Intersects With	Component Duplication Avoidance	AST-02.3	Mechanisms exist to establish and maintain an authoritative source and repository to provide a trusted source and accountability for approved and implemented system components that prevents assets from being duplicated in other asset inventories.	5		Low
CM-08(01)	System Component Inventory | Updates During Installation and Removal	Update the inventory of system components as part of component installations, removals, and system updates.	Functional	Equal	Updates During Installations / Removals	AST-02.1	Mechanisms exist to update asset inventories as part of component installations, removals and asset upgrades.	10		Moderate

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-53B Baseline
CM-08(02)	System Component Inventory | Automated Maintenance	Maintain the currency, completeness, accuracy, and availability of the inventory of system components using [Assignment: organization-defined automated mechanisms].	Functional	Equal	Configuration Management Database (CMDB)	AST-02.9	Mechanisms exist to implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific information.	10		High
CM-08(03)	System Component Inventory | Automated Unauthorized Component Detection	a. Detect the presence of unauthorized hardware, software, and firmware components within the system using [Assignment: organization-defined automated mechanisms] [Assignment: organization-defined frequency]; andb. Take the following actions when unauthorized components are detected: [Selection (one or more): disable network access by such components; isolate the components; notify [Assignment: organization-defined personnel or roles]].	Functional	Intersects With	Automated Unauthorized Component Detection	AST-02.2	Automated mechanisms exist to detect and alert upon the detection of unauthorized hardware, software and firmware components.	5		Moderate
CM-08(03)	System Component Inventory | Automated Unauthorized Component Detection	a. Detect the presence of unauthorized hardware, software, and firmware components within the system using [Assignment: organization-defined automated mechanisms] [Assignment: organization-defined frequency]; andb. Take the following actions when unauthorized components are detected: [Selection (one or more): disable network access by such components; isolate the components; notify [Assignment: organization-defined personnel or roles]].	Functional	Intersects With	Software Installation Alerts	END-03.1	Mechanisms exist to generate an alert when new software is detected.	5		Moderate
CM-08(03)	System Component Inventory | Automated Unauthorized Component Detection	a. Detect the presence of unauthorized hardware, software, and firmware components within the system using [Assignment: organization-defined automated mechanisms] [Assignment: organization-defined frequency]; andb. Take the following actions when unauthorized components are detected: [Selection (one or more): disable network access by such components; isolate the components; notify [Assignment: organization-defined personnel or roles]].	Functional	Intersects With	Unauthorized Installation Alerts	CFG-05.1	Mechanisms exist to configure systems to generate an alert when the unauthorized installation of software is detected.	5		Moderate
CM-08(04)	System Component Inventory | Accountability Information	Include in the system component inventory information, a means for identifying by [Selection (one or more): name; position; role], individuals responsible and accountable for administering those components.	Functional	Equal	Accountability Information	AST-03.1	Mechanisms exist to include capturing the name, position and/or role of individuals responsible/accountable for administering assets as part of the technology asset inventory process.	10		High
CM-08(05)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
CM-08(06)	System Component Inventory | Assessed Configurations and Approved Deviations	Include assessed component configurations and any approved deviations to current deployed configurations in the system component inventory.	Functional	Equal	Approved Baseline Deviations	AST-02.4	Mechanisms exist to document and govern instances of approved deviations from established baseline configurations.	10		Not Selected
CM-08(07)	System Component Inventory | Centralized Repository	Provide a centralized repository for the inventory of system components.	Functional	Intersects With	Configuration Management Database (CMDB)	AST-02.9	Mechanisms exist to implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific information.	5		Not Selected
CM-08(08)	System Component Inventory | Automated Location Tracking	Support the tracking of system components by geographic location using [Assignment: organization-defined automated mechanisms].	Functional	Equal	Automated Location Tracking	AST-02.10	Mechanisms exist to track the geographic location of system components.	10		Not Selected
CM-08(09)	System Component Inventory | Assignment of Components to Systems	a. Assign system components to a system; andb. Receive an acknowledgement from [Assignment: organization-defined personnel or roles] of this assignment.	Functional	Equal	Component Assignment	AST-02.11	Mechanisms exist to bind components to a specific system.	10		Not Selected
CM-09	Configuration Management Plan	Develop, document, and implement a configuration management plan for the system that:a. Addresses roles, responsibilities, and configuration management processes and procedures;b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;c. Defines the configuration items for the system and places the configuration items under configuration management;d. Is reviewed and approved by [Assignment: organization-defined personnel or roles]; ande. Protects the configuration management plan from unauthorized disclosure and modification.	Functional	Subset Of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10		Moderate
CM-09	Configuration Management Plan	Develop, document, and implement a configuration management plan for the system that:a. Addresses roles, responsibilities, and configuration management processes and procedures;b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;c. Defines the configuration items for the system and places the configuration items under configuration management;d. Is reviewed and approved by [Assignment: organization-defined personnel or roles]; ande. Protects the configuration management plan from unauthorized disclosure and modification.	Functional	Intersects With	Stakeholder Notification of Changes	CHG-05	Mechanisms exist to ensure stakeholders are made aware of and understand the impact of proposed changes.	5		Moderate
CM-09(01)	Configuration Management Plan | Assignment of Responsibility	Assign responsibility for developing the configuration management process to organizational personnel that are not directly involved in system development.	Functional	Equal	Assignment of Responsibility	CFG-01.1	Mechanisms exist to implement a segregation of duties for configuration management that prevents developers from performing production configuration management duties.	10		Not Selected
CM-10	Software Usage Restrictions	a. Use software and associated documentation in accordance with contract agreements and copyright laws;b. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; andc. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.	Functional	Equal	Software Usage Restrictions	CFG-04	Mechanisms exist to enforce software usage restrictions to comply with applicable contract agreements and copyright laws.	10		Low
CM-10(01)	Software Usage Restrictions | Open-source Software	Establish the following restrictions on the use of open-source software: [Assignment: organization-defined restrictions].	Functional	Equal	Open Source Software	CFG-04.1	Mechanisms exist to establish parameters for the secure use of open source software.	10		Not Selected
CM-11	User-installed Software	a. Establish [Assignment: organization-defined policies] governing the installation of software by users;b. Enforce software installation policies through the following methods: [Assignment: organization-defined methods]; andc. Monitor policy compliance [Assignment: organization-defined frequency].	Functional	Intersects With	Prohibit Installation Without Privileged Status	END-03	Automated mechanisms exist to prohibit software installations without explicitly assigned privileged status.	5		Low
CM-11	User-installed Software	a. Establish [Assignment: organization-defined policies] governing the installation of software by users;b. Enforce software installation policies through the following methods: [Assignment: organization-defined methods]; andc. Monitor policy compliance [Assignment: organization-defined frequency].	Functional	Intersects With	User-Installed Software	CFG-05	Mechanisms exist to restrict the ability of non-privileged users to install unauthorized software.	5		Low
CM-11(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
CM-11(02)	User-installed Software | Software Installation with Privileged Status	Allow user installation of software only with explicit privileged status.	Functional	Intersects With	User-Installed Software	CFG-05	Mechanisms exist to restrict the ability of non-privileged users to install unauthorized software.	5		Not Selected
CM-11(02)	User-installed Software | Software Installation with Privileged Status	Allow user installation of software only with explicit privileged status.	Functional	Intersects With	Restrict Roles Permitted To Install Software	CFG-05.2	Mechanisms exist to configure systems to prevent the installation of software, unless the action is performed by a privileged user or service.	5		Not Selected
CM-11(02)	User-installed Software | Software Installation with Privileged Status	Allow user installation of software only with explicit privileged status.	Functional	Intersects With	Prohibit Installation Without Privileged Status	END-03	Automated mechanisms exist to prohibit software installations without explicitly assigned privileged status.	5		Not Selected
CM-11(03)	User-installed Software | Automated Enforcement and Monitoring	Enforce and monitor compliance with software installation policies using [Assignment: organization-defined automated mechanisms].	Functional	Intersects With	Configuration Enforcement	CFG-06	Automated mechanisms exist to monitor, enforce and report on configurations for endpoint devices.	5		Not Selected
CM-11(03)	User-installed Software | Automated Enforcement and Monitoring	Enforce and monitor compliance with software installation policies using [Assignment: organization-defined automated mechanisms].	Functional	Intersects With	Integrity Assurance & Enforcement (IAE)	CFG-06.1	Automated mechanisms exist to identify unauthorized deviations from an approved baseline and implement automated resiliency actions to remediate the unauthorized change.	5		Not Selected
CM-11(03)	User-installed Software | Automated Enforcement and Monitoring	Enforce and monitor compliance with software installation policies using [Assignment: organization-defined automated mechanisms].	Functional	Intersects With	Software Installation Alerts	END-03.1	Mechanisms exist to generate an alert when new software is detected.	5		Not Selected

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh	Notes	NIST SP 800-53B Baseline
CM-11(03)	User-installed Software | Automated Enforcement and Monitoring	Enforce and monitor compliance with software installation policies using [Assignment: organization-defined automated mechanisms].	Functional	Intersects With	Unauthorized Installation Alerts	CFG-05.1	Mechanisms exist to configure systems to generate an alert when the unauthorized installation of software is detected.	5		Not Selected
CM-12	Information Location	a. Identify and document the location of [Assignment: organization-defined information] and the specific system components on which the information is processed and stored;b. Identify and document the users who have access to the system and system components where the information is processed and stored; andc. Document changes to the location (i.e., system or system components) where the information is processed and stored.	Functional	Equal	Information Location	DCH-24	Mechanisms exist to identify and document the location of information and the specific system components on which the information resides.	10		Moderate
CM-12(01)	Information Location | Automated Tools to Support Information Location	Use automated tools to identify [Assignment: organization-defined information by information type] on [Assignment: organization-defined system components] to ensure controls are in place to protect organizational information and individual privacy.	Functional	Equal	Automated Tools to Support Information Location	DCH-24.1	Automated mechanisms exist to identify by data classification type to ensure adequate security, compliance and resilience controls are in place to protect organizational information and individual data protection.	10		Moderate
CM-13	Data Action Mapping	Develop and document a map of system data actions.	Functional	Equal	Data Action Mapping	AST-02.8	Mechanisms exist to create and maintain a map of Technology Assets, Applications and/or Services (TAAS) where sensitive/regulated data is stored, transmitted or processed.	10		Not Selected
CM-14	Signed Components	Prevent the installation of [Assignment: organization-defined software and firmware components] without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.	Functional	Intersects With	Signed Components	CHG-04.2	Mechanisms exist to prevent the installation of software and firmware components without verification that the component has been digitally signed using an organization-approved certificate authority.	5		Not Selected
CP-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] contingency planning policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the contingency planning policy and the associated contingency planning controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the contingency planning policy and procedures; andc. Review and update the current contingency planning:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5		Low
CP-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] contingency planning policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the contingency planning policy and the associated contingency planning controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the contingency planning policy and procedures; andc. Review and update the current contingency planning:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10		Low
CP-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] contingency planning policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the contingency planning policy and the associated contingency planning controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the contingency planning policy and procedures; andc. Review and update the current contingency planning:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5		Low
CP-02	Contingency Plan	a. Develop a contingency plan for the system that:1. Identifies essential mission and business functions and associated contingency requirements;2. Provides recovery objectives, restoration priorities, and metrics;3. Addresses contingency roles, responsibilities, assigned individuals with contact information;4. Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure;5. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented;6. Addresses the sharing of contingency information; and7. Is reviewed and approved by [Assignment: organization-defined personnel or roles];b. Distribute copies of the contingency plan to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements];c. Coordinate contingency planning activities with incident handling activities;d. Review the contingency plan for the system [Assignment: organization-defined frequency];e. Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;f. Communicate contingency plan changes to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements];g. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training; andh. Protect the contingency plan from unauthorized disclosure and modification.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10		Low

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-53B Baseline
CP-02	Contingency Plan	a. Develop a contingency plan for the system that:1. Identifies essential mission and business functions and associated contingency requirements;2. Provides recovery objectives, restoration priorities, and metrics;3. Addresses contingency roles, responsibilities, assigned individuals with contact information;4. Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure;5. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented;6. Addresses the sharing of contingency information; and7. Is reviewed and approved by [Assignment: organization-defined personnel or roles];b. Distribute copies of the contingency plan to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements];c. Coordinate contingency planning activities with incident handling activities;d. Review the contingency plan for the system [Assignment: organization-defined frequency];e. Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;f. Communicate contingency plan changes to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements];g. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training; andh. Protect the contingency plan from unauthorized disclosure and modification.	Functional	Intersects With	Ongoing Contingency Planning	BCD-06	Mechanisms exist to update contingency plans due to changes affecting: (1) People (e.g., personnel changes); (2) Processes (e.g., new, altered or decommissioned business practices, including third-party services) (3) Technologies (e.g., new, altered or decommissioned technologies); (4) Data (e.g., changes to data flows and/or data repositories); (5) Facilities (e.g., new, altered or decommissioned physical infrastructure); and/or (6) Feedback from contingency plan testing activities.	5		Low
CP-02(01)	Contingency Plan | Coordinate with Related Plans	Coordinate contingency plan development with organizational elements responsible for related plans.	Functional	Equal	Coordinate with Related Plans	BCD-01.1	Mechanisms exist to coordinate contingency plan development with internal and external elements responsible for related plans.	10		Moderate
CP-02(02)	Contingency Plan | Capacity Planning	Conduct capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.	Functional	Equal	Capacity Planning	CAP-03	Mechanisms exist to conduct capacity planning so that necessary capacity for information processing, telecommunications and environmental support will exist during contingency operations.	10		High
CP-02(03)	Contingency Plan | Resume Mission and Business Functions	Plan for the resumption of [Selection (one): all; essential] mission and business functions within [Assignment: organization-defined time period] of contingency plan activation.	Functional	Intersects With	Resume All Missions & Business Functions	BCD-02.1	Mechanisms exist to resume all missions and business functions within Recovery Time Objectives (RTOs) of the contingency plan's activation.	5		Moderate
CP-02(03)	Contingency Plan | Resume Mission and Business Functions	Plan for the resumption of [Selection (one): all; essential] mission and business functions within [Assignment: organization-defined time period] of contingency plan activation.	Functional	Intersects With	Resume Essential Missions & Business Functions	BCD-02.3	Mechanisms exist to resume essential missions and business functions within an organization-defined time period of contingency plan activation.	5		Moderate
CP-02(04)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
CP-02(05)	Contingency Plan | Continue Mission and Business Functions	Plan for the continuance of [Selection (one): all; essential] mission and business functions with minimal or no loss of operational continuity and sustains that continuity until full system restoration at primary processing and/or storage sites.	Functional	Equal	Continue Essential Mission & Business Functions	BCD-02.2	Mechanisms exist to continue essential missions and business functions with little or no loss of operational continuity and sustain that continuity until full system restoration at primary processing and/or storage sites.	10		High
CP-02(06)	Contingency Plan | Alternate Processing and Storage Sites	Plan for the transfer of [Selection (one): all; essential] mission and business functions to alternate processing and/or storage sites with minimal or no loss of operational continuity and sustain that continuity through system restoration to primary processing and/or storage sites.	Functional	Equal	Transfer to Alternate Processing / Storage Site	BCD-01.3	Mechanisms exist to redeploy personnel to other roles during a disruptive event or in the execution of a continuity plan.	10		Not Selected
CP-02(07)	Contingency Plan | Coordinate with External Service Providers	Coordinate the contingency plan with the contingency plans of external service providers to ensure that contingency requirements can be satisfied.	Functional	Equal	Coordinate With External Service Providers	BCD-01.2	Mechanisms exist to coordinate internal contingency plans with the contingency plans of external service providers to ensure that contingency requirements can be satisfied.	10		Not Selected
CP-02(08)	Contingency Plan | Identify Critical Assets	Identify critical system assets supporting [Selection (one): all; essential] mission and business functions.	Functional	Equal	Identify Critical Assets	BCD-02	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions.	10		Moderate
CP-03	Contingency Training	a. Provide contingency training to system users consistent with assigned roles and responsibilities:1. Within [Assignment: organization-defined time period] of assuming a contingency role or responsibility;2. When required by system changes; and3. [Assignment: organization-defined frequency] thereafter; andb. Review and update contingency training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Equal	Contingency Training	BCD-03	Mechanisms exist to adequately train contingency personnel and applicable stakeholders in their contingency roles and responsibilities.	10		Low
CP-03(01)	Contingency Training | Simulated Events	Incorporate simulated events into contingency training to facilitate effective response by personnel in crisis situations.	Functional	Equal	Simulated Events	BCD-03.1	Mechanisms exist to incorporate simulated events into contingency training to facilitate effective response by personnel in crisis situations.	10		High
CP-03(02)	Contingency Training | Mechanisms Used in Training Environments	Employ mechanisms used in operations to provide a more thorough and realistic contingency training environment.	Functional	Equal	Automated Training Environments	BCD-03.2	Automated mechanisms exist to provide a more thorough and realistic contingency training environment.	10		Not Selected
CP-04	Contingency Plan Testing	a. Test the contingency plan for the system [Assignment: organization-defined frequency] using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: [Assignment: organization-defined tests].b. Review the contingency plan test results; andc. Initiate corrective actions, if needed.	Functional	Intersects With	Contingency Plan Root Cause Analysis (RCA) & Lessons Learned	BCD-05	Mechanisms exist to conduct a Root Cause Analysis (RCA) and "lessons learned" activity every time the contingency plan is activated.	5		Low
CP-04	Contingency Plan Testing	a. Test the contingency plan for the system [Assignment: organization-defined frequency] using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: [Assignment: organization-defined tests].b. Review the contingency plan test results; andc. Initiate corrective actions, if needed.	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	5		Low
CP-04(01)	Contingency Plan Testing | Coordinate with Related Plans	Coordinate contingency plan testing with organizational elements responsible for related plans.	Functional	Equal	Coordinated Testing with Related Plans	BCD-04.1	Mechanisms exist to coordinate contingency plan testing with internal and external elements responsible for related plans.	10		Moderate
CP-04(02)	Contingency Plan Testing | Alternate Processing Site	Test the contingency plan at the alternate processing site:a. To familiarize contingency personnel with the facility and available resources; andb. To evaluate the capabilities of the alternate processing site to support contingency operations.	Functional	Equal	Alternate Storage & Processing Sites	BCD-04.2	Mechanisms exist to test contingency plans at alternate storage & processing sites to both familiarize contingency personnel with the facility and evaluate the capabilities of the alternate processing site to support contingency operations.	10		High
CP-04(03)	Contingency Plan Testing | Automated Testing	Test the contingency plan using [Assignment: organization-defined automated mechanisms].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
CP-04(04)	Contingency Plan Testing | Full Recovery and Reconstitution	Include a full recovery and reconstitution of the system to a known state as part of contingency plan testing.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
CP-04(05)	Contingency Plan Testing | Self-challenge	Employ [Assignment: organization-defined mechanisms] to [Assignment: organization-defined system or system component] to disrupt and adversely affect the system or system component.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
CP-05		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
CP-06	Alternate Storage Site	a. Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information; andb. Ensure that the alternate storage site provides controls equivalent to that of the primary site.	Functional	Equal	Alternate Storage Site	BCD-08	Mechanisms exist to establish an alternate storage site that includes both the assets and necessary agreements to permit the storage and recovery of system backup information.	10		Moderate
CP-06(01)	Alternate Storage Site | Separation from Primary Site	Identify an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats.	Functional	Equal	Separation from Primary Storage Site	BCD-08.1	Mechanisms exist to separate the alternate storage site from the primary storage site to reduce susceptibility to similar threats.	10		Moderate

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-53B Baseline
CP-06(02)	Alternate Storage Site | Recovery Time and Recovery Point Objectives	Configure the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.	Functional	Intersects With	Recovery Time / Point Objectives (RTO / RPO)	BCD-01.4	Mechanisms exist to facilitate recovery operations in accordance with Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5		High
CP-06(03)	Alternate Storage Site | Accessibility	Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.	Functional	Equal	Primary Storage Site Accessibility	BCD-08.2	Mechanisms exist to identify and mitigate potential accessibility problems to the alternate storage sites in the event of an area-wide disruption or disaster.	10		Moderate
CP-07	Alternate Processing Site	a. Establish an alternate processing site, including necessary agreements to permit the transfer and resumption of [Assignment: organization-defined system operations] for essential mission and business functions within [Assignment: organization-defined time period consistent with recovery time and recovery point objectives] when the primary processing capabilities are unavailable;b. Make available at the alternate processing site, the equipment and supplies required to transfer and resume operations or put contracts in place to support delivery to the site within the organization-defined time period for transfer and resumption; andc. Provide controls at the alternate processing site that are equivalent to those at the primary site.	Functional	Equal	Alternate Processing Site	BCD-09	Mechanisms exist to establish an alternate processing site that provides security measures equivalent to that of the primary site.	10		Moderate
CP-07(01)	Alternate Processing Site | Separation from Primary Site	Identify an alternate processing site that is sufficiently separated from the primary processing site to reduce susceptibility to the same threats.	Functional	Equal	Separation from Primary Processing Site	BCD-09.1	Mechanisms exist to separate the alternate processing site from the primary processing site to reduce susceptibility to similar threats.	10		Moderate
CP-07(02)	Alternate Processing Site | Accessibility	Identify potential accessibility problems to alternate processing sites in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.	Functional	Equal	Alternate Processing Site Accessibility	BCD-09.2	Mechanisms exist to identify and mitigate potential accessibility problems to the alternate processing sites and possible mitigation actions, in the event of an area-wide disruption or disaster.	10		Moderate
CP-07(03)	Alternate Processing Site | Priority of Service	Develop alternate processing site agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives).	Functional	Equal	Alternate Site Priority of Service	BCD-09.3	Mechanisms exist to address priority-of-service provisions in alternate processing and storage sites that support availability requirements, including Recovery Time Objectives (RTOs).	10		Moderate
CP-07(04)	Alternate Processing Site | Preparation for Use	Prepare the alternate processing site so that the site can serve as the operational site supporting essential mission and business functions.	Functional	Equal	Preparation for Use	BCD-09.4	Mechanisms exist to prepare the alternate processing alternate to support essential missions and business functions so that the alternate site is capable of being used as the primary site.	10		High
CP-07(05)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
CP-07(06)	Alternate Processing Site | Inability to Return to Primary Site	Plan and prepare for circumstances that preclude returning to the primary processing site.	Functional	Equal	Inability to Return to Primary Site	BCD-09.5	Mechanisms exist to plan and prepare for both natural and manmade circumstances that preclude returning to the primary site.	10		Not Selected
CP-08	Telecommunications Services	Establish alternate telecommunications services, including necessary agreements to permit the resumption of [Assignment: organization-defined system operations] for essential mission and business functions within [Assignment: organization-defined time period] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.	Functional	Intersects With	Telecommunications Services Availability	BCD-10	Mechanisms exist to reduce the likelihood of a single point of failure with primary telecommunications services.	5		Moderate
CP-08(01)	Telecommunications Services | Priority of Service Provisions	a. Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives); andb. Request Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness if the primary and/or alternate telecommunications services are provided by a common carrier.	Functional	Equal	Telecommunications Priority of Service Provisions	BCD-10.1	Mechanisms exist to formalize primary and alternate telecommunications service agreements contain priority-of-service provisions that support availability requirements, including Recovery Time Objectives (RTOs).	10		Moderate
CP-08(02)	Telecommunications Services | Single Points of Failure	Obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.	Functional	Intersects With	Telecommunications Services Availability	BCD-10	Mechanisms exist to reduce the likelihood of a single point of failure with primary telecommunications services.	5		Moderate
CP-08(03)	Telecommunications Services | Separation of Primary and Alternate Providers	Obtain alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.	Functional	Equal	Separation of Primary / Alternate Providers	BCD-10.2	Mechanisms exist to obtain alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.	10		High
CP-08(04)	Telecommunications Services | Provider Contingency Plan	a. Require primary and alternate telecommunications service providers to have contingency plans;b. Review provider contingency plans to ensure that the plans meet organizational contingency requirements; andc. Obtain evidence of contingency testing and training by providers [Assignment: organization-defined frequency].	Functional	Equal	Provider Contingency Plan	BCD-10.3	Mechanisms exist to contractually-require external service providers to have contingency plans that meet organizational contingency requirements.	10		High
CP-08(05)	Telecommunications Services | Alternate Telecommunication Service Testing	Test alternate telecommunication services [Assignment: organization-defined frequency].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
CP-09	System Backup	a. Conduct backups of user-level information contained in [Assignment: organization-defined system components] [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives];b. Conduct backups of system-level information contained in the system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives];c. Conduct backups of system documentation, including security- and privacy-related documentation [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; andd. Protect the confidentiality, integrity, and availability of backup information.	Functional	Intersects With	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5		Low
CP-09(01)	System Backup | Testing for Reliability and Integrity	Test backup information [Assignment: organization-defined frequency] to verify media reliability and information integrity.	Functional	Equal	Testing for Reliability & Integrity	BCD-11.1	Mechanisms exist to routinely test backups that verify the reliability of the backup process, as well as the integrity and availability of the data.	10		Moderate
CP-09(02)	System Backup | Test Restoration Using Sampling	Use a sample of backup information in the restoration of selected system functions as part of contingency plan testing.	Functional	Equal	Test Restoration Using Sampling	BCD-11.5	Mechanisms exist to utilize sampling of available backups to test recovery capabilities as part of business continuity plan testing.	10		High
CP-09(03)	System Backup | Separate Storage for Critical Information	Store backup copies of [Assignment: organization-defined critical system software and other security-related information] in a separate facility or in a fire rated container that is not collocated with the operational system.	Functional	Equal	Separate Storage for Critical Information	BCD-11.2	Mechanisms exist to store backup copies of critical software and other security-related information in a separate facility or in a fire-rated container that is not collocated with the system being backed up.	10		High
CP-09(04)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
CP-09(05)	System Backup | Transfer to Alternate Storage Site	Transfer system backup information to the alternate storage site [Assignment: organization-defined time period and transfer rate consistent with the recovery time and recovery point objectives].	Functional	Equal	Transfer to Alternate Storage Site	BCD-11.6	Mechanisms exist to transfer backup data to the alternate storage site at a rate that is capable of meeting both Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	10		High
CP-09(06)	System Backup | Redundant Secondary System	Conduct system backup by maintaining a redundant secondary system that is not collocated with the primary system and that can be activated without loss of information or disruption to operations.	Functional	Equal	Redundant Secondary System	BCD-11.7	Mechanisms exist to maintain a failover capability, which is not collocated with the primary Technology Asset, Application and/or Service (TAAS), which can be activated with little-to-no loss of information or disruption to operations.	10		Not Selected
CP-09(07)	System Backup | Dual Authorization for Deletion or Destruction	Enforce dual authorization for the deletion or destruction of [Assignment: organization-defined backup information].	Functional	Equal	Dual Authorization For Backup Media Destruction	BCD-11.8	Mechanisms exist to implement and enforce dual authorization for the deletion or destruction of sensitive backup media and data.	10		Not Selected

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-53B Baseline
CP-09(08)	System Backup | Cryptographic Protection	Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of [Assignment: organization-defined backup information].	Functional	Equal	Cryptographic Protection	BCD-11.4	Cryptographic mechanisms exist to prevent the unauthorized disclosure and/or modification of backup information.	10		Moderate
CP-10	System Recovery and Reconstitution	Provide for the recovery and reconstitution of the system to a known state within [Assignment: organization-defined time period consistent with recovery time and recovery point objectives] after a disruption, compromise, or failure.	Functional	Intersects With	Technology Assets, Applications and/or Services (TAAS) Recovery & Reconstitution	BCD-12	Mechanisms exist to ensure the secure recovery and reconstitution of Technology Assets, Applications and/or Services (TAAS) to a known state after a disruption, compromise or	5		Low
CP-10	System Recovery and Reconstitution	Provide for the recovery and reconstitution of the system to a known state within [Assignment: organization-defined time period consistent with recovery time and recovery point objectives] after a disruption, compromise, or failure.	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	5		Low
CP-10	System Recovery and Reconstitution	Provide for the recovery and reconstitution of the system to a known state within [Assignment: organization-defined time period consistent with recovery time and recovery point objectives] after a disruption, compromise, or failure.	Functional	Intersects With	Recovery Time / Point Objectives (RTO / RPO)	BCD-01.4	Mechanisms exist to facilitate recovery operations in accordance with Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5		Low
CP-10(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
CP-10(02)	System Recovery and Reconstitution | Transaction Recovery	Implement transaction recovery for systems that are transaction-based.	Functional	Equal	Transaction Recovery	BCD-12.1	Mechanisms exist to utilize specialized backup mechanisms that will allow transaction recovery for transaction-based Technology Assets, Applications and/or Services (TAAS) in accordance with Recovery Point	10		Moderate
CP-10(03)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
CP-10(04)	System Recovery and Reconstitution | Restore Within Time Period	Provide the capability to restore system components within [Assignment: organization-defined restoration time periods] from configuration-controlled and integrity-protected information representing a known, operational state for the components.	Functional	Equal	Restore Within Time Period	BCD-12.4	Mechanisms exist to restore Technology Assets, Applications, Services and/or Data (TAASD) within organization-defined restoration time-periods from configuration-controlled and integrity-protected information; representing a known,	10		High
CP-10(05)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
CP-10(06)	System Recovery and Reconstitution | Component Protection	Protect system components used for recovery and reconstitution.	Functional	Equal	Backup & Restoration Hardware Protection	BCD-13	Mechanisms exist to protect backup and restoration hardware and software.	10		Not Selected
CP-11	Alternate Communications Protocols	Provide the capability to employ [Assignment: organization-defined alternative communications protocols] in support of maintaining continuity of operations.	Functional	Intersects With	Telecommunications Services Availability	BCD-10	Mechanisms exist to reduce the likelihood of a single point of failure with primary telecommunications services.	5		Not Selected
CP-12	Safe Mode	When [Assignment: organization-defined conditions] are detected, enter a safe mode of operation with [Assignment: organization-defined restrictions of safe mode of operation].	Functional	Intersects With	Fail Secure	SEA-07.2	Mechanisms exist to cause systems to fail to an organization-defined known-state for types of failures, preserving system state information in	5		Not Selected
CP-13	Alternative Security Mechanisms	Employ [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.	Functional	Equal	Alternative Security Measures	BCD-07	Mechanisms exist to implement alternative or compensating controls to satisfy security functions when the primary means of implementing the security function is unavailable or compromised.	10		Not Selected
IA-01	Policy and Procedures	[Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] identification and authentication policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the identification and authentication policy and procedures; andc. Review and update the current identification and authentication:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5		Low
IA-01	Policy and Procedures	[Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] identification and authentication policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the identification and authentication policy and procedures; andc. Review and update the current identification and authentication:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10		Low
IA-01	Policy and Procedures	[Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] identification and authentication policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the identification and authentication policy and procedures; andc. Review and update the current identification and authentication:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5		Low
IA-02	Identification and Authentication (organizational Users)	Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.	Functional	Equal	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	10		Low

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-53B Baseline
IA-02(01)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts	Implement multi-factor authentication for access to privileged accounts.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulated data.	5		Low
IA-02(01)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts	Implement multi-factor authentication for access to privileged accounts.	Functional	Intersects With	Local Access to Privileged Accounts	IAC-06.3	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate local access for privileged accounts.	5		Low
IA-02(01)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts	Implement multi-factor authentication for access to privileged accounts.	Functional	Intersects With	Information Assurance Enabled Products	TDA-02.2	Mechanisms exist to limit the use of commercially-provided Information Assurance (IA) and IA-enabled IT products to those products that have been successfully evaluated against a National Information Assurance partnership (NIAP)-approved Protection Profile or the cryptographic module is FIPS-validated or NSA-approved.	5		Low
IA-02(01)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts	Implement multi-factor authentication for access to privileged accounts.	Functional	Intersects With	Out-of-Band Multi-Factor Authentication	IAC-06.4	Mechanisms exist to implement Multi-Factor Authentication (MFA) for access to privileged and non-privileged accounts such that one of the factors is independently provided by a device separate from the system being accessed.	5		Low
IA-02(01)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts	Implement multi-factor authentication for access to privileged accounts.	Functional	Intersects With	Network Access to Privileged Accounts	IAC-06.1	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for privileged accounts.	5		Low
IA-02(01)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts	Implement multi-factor authentication for access to privileged accounts.	Functional	Intersects With	Network Access to Non-Privileged Accounts	IAC-06.2	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for non-privileged accounts.	5		Low
IA-02(01)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts	Implement multi-factor authentication for access to privileged accounts.	Functional	Intersects With	Hardware Token-Based Authentication	IAC-10.7	Automated mechanisms exist to ensure organization-defined token quality requirements are satisfied for hardware token-based authentication.	5		Low
IA-02(02)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Non-privileged Accounts	Implement multi-factor authentication for access to non-privileged accounts.	Functional	Intersects With	Information Assurance Enabled Products	TDA-02.2	Mechanisms exist to limit the use of commercially-provided Information Assurance (IA) and IA-enabled IT products to those products that have been successfully evaluated against a National Information Assurance partnership (NIAP)-approved Protection Profile or the cryptographic module is FIPS-validated or NSA-approved.	5		Low
IA-02(02)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Non-privileged Accounts	Implement multi-factor authentication for access to non-privileged accounts.	Functional	Intersects With	Network Access to Non-Privileged Accounts	IAC-06.2	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for non-privileged accounts.	5		Low
IA-02(02)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Non-privileged Accounts	Implement multi-factor authentication for access to non-privileged accounts.	Functional	Intersects With	Out-of-Band Multi-Factor Authentication	IAC-06.4	Mechanisms exist to implement Multi-Factor Authentication (MFA) for access to privileged and non-privileged accounts such that one of the factors is independently provided by a device separate from the system being accessed.	5		Low
IA-02(02)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Non-privileged Accounts	Implement multi-factor authentication for access to non-privileged accounts.	Functional	Intersects With	Hardware Token-Based Authentication	IAC-10.7	Automated mechanisms exist to ensure organization-defined token quality requirements are satisfied for hardware token-based authentication.	5		Low
IA-02(02)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Non-privileged Accounts	Implement multi-factor authentication for access to non-privileged accounts.	Functional	Intersects With	Network Access to Privileged Accounts	IAC-06.1	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for privileged accounts.	5		Low
IA-02(02)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Non-privileged Accounts	Implement multi-factor authentication for access to non-privileged accounts.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulated data.	5		Low
IA-02(02)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Non-privileged Accounts	Implement multi-factor authentication for access to non-privileged accounts.	Functional	Intersects With	Local Access to Privileged Accounts	IAC-06.3	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate local access for privileged accounts.	5		Low
IA-02(03)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
IA-02(04)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
IA-02(05)	Identification and Authentication (organizational Users) | Individual Authentication with Group Authentication	When shared accounts or authenticators are employed, require users to be individually authenticated before granting access to the shared accounts or resources.	Functional	Equal	Group Authentication	IAC-02.1	Mechanisms exist to require individuals to be authenticated with an individual authenticator when a group authenticator is utilized.	10		High
IA-02(06)	Identification and Authentication (organizational Users) | Access to Accounts — separate Device	Implement multi-factor authentication for [Selection (one or more): local; network; remote] access to [Selection (one or more): privileged accounts; non-privileged accounts] such that:a. One of the factors is provided by a device separate from the system gaining access; andb. The device meets [Assignment: organization-defined strength of mechanism requirements].	Functional	Intersects With	Out-of-Band Multi-Factor Authentication	IAC-06.4	Mechanisms exist to implement Multi-Factor Authentication (MFA) for access to privileged and non-privileged accounts such that one of the factors is independently provided by a device separate from the system being accessed.	5		Not Selected
IA-02(07)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
IA-02(08)	Identification and Authentication (organizational Users) | Access to Accounts — Replay Resistant	Implement replay-resistant authentication mechanisms for access to [Selection (one or more): privileged accounts; non-privileged accounts].	Functional	Equal	Replay-Resistant Authentication	IAC-02.2	Automated mechanisms exist to employ replay-resistant authentication.	10		Low

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-53B Baseline
IA-02(09)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
IA-02(10)	Identification and Authentication (organizational Users) | Single Sign-on	Provide a single sign-on capability for [Assignment: organization-defined system accounts and services].	Functional	Equal	Single Sign-On (SSO) Transparent Authentication	IAC-13.1	Mechanisms exist to provide a transparent authentication (e.g., Single Sign-On (SSO)) capability to the organization's Technology Assets, Applications and/or Services (TAAS).	10		Not Selected
IA-02(11)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
IA-02(12)	Identification and Authentication (organizational Users) | Acceptance of PIV Credentials	Accept and electronically verify Personal Identity Verification-compliant credentials.	Functional	Intersects With	Acceptance of PIV Credentials	IAC-02.3	Mechanisms exist to accept and electronically verify organizational Personal Identity Verification (PIV) credentials.	5		Low
IA-02(13)	Identification and Authentication (organizational Users) | Out-of-band Authentication	Implement the following out-of-band authentication mechanisms under [Assignment: organization-defined conditions]: [Assignment: organization-defined out-of-band authentication].	Functional	Equal	Out-of-Band Authentication (OOBA)	IAC-02.4	Mechanisms exist to implement Out-of-Band Authentication (OOBA) under specific conditions.	10		Not Selected
IA-03	Device Identification and Authentication	Uniquely identify and authenticate [Assignment: organization-defined devices and/or types of devices] before establishing a [Selection (one or more): local; remote; network] connection.	Functional	Intersects With	Identification & Authentication for Devices	IAC-04	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional authentication that is cryptographically- based and replay resistant.	5		Moderate
IA-03(01)	Device Identification and Authentication | Cryptographic Bidirectional Authentication	Authenticate [Assignment: organization-defined devices and/or types of devices] before establishing [Selection (one or more): local; remote; network] connection using bidirectional authentication that is cryptographically based.	Functional	Intersects With	Identification & Authentication for Devices	IAC-04	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional authentication that is cryptographically- based and replay resistant.	5		Not Selected
IA-03(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
IA-03(03)	Device Identification and Authentication | Dynamic Address Allocation	a. Where addresses are allocated dynamically, standardize dynamic address allocation lease information and the lease duration assigned to devices in accordance with [Assignment: organization-defined lease information and lease duration]; andb. Audit lease information when assigned to a device.	Functional	Intersects With	Network Access Control (NAC)	AST-02.5	Automated mechanisms exist to employ Network Access Control (NAC), or a similar technology, which is capable of detecting unauthorized devices and disable network access to those unauthorized devices.	5		Not Selected
IA-03(04)	Device Identification and Authentication | Device Attestation	Handle device identification and authentication based on attestation by [Assignment: organization-defined configuration management process].	Functional	Intersects With	Identification & Authentication for Devices	IAC-04	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional authentication that is cryptographically- based and replay resistant.	5		Not Selected
IA-03(04)	Device Identification and Authentication | Device Attestation	Handle device identification and authentication based on attestation by [Assignment: organization-defined configuration management process].	Functional	Intersects With	Device Attestation	IAC-04.1	Mechanisms exist to ensure device identification and authentication is accurate by centrally-managing the joining of systems to the domain as part of the initial asset configuration management process.	5		Not Selected
IA-04	Identifier Management	Manage system identifiers by:a. Receiving authorization from [Assignment: organization-defined personnel or roles] to assign an individual, group, role, service, or device identifier;b. Selecting an identifier that identifies an individual, group, role, service, or device;c. Assigning the identifier to the intended individual, group, role, service, or device; andd. Preventing reuse of identifiers for [Assignment: organization-defined time period].	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAC-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	5		Low
IA-04	Identifier Management	Manage system identifiers by:a. Receiving authorization from [Assignment: organization-defined personnel or roles] to assign an individual, group, role, service, or device identifier;b. Selecting an identifier that identifies an individual, group, role, service, or device;c. Assigning the identifier to the intended individual, group, role, service, or device; andd. Preventing reuse of identifiers for [Assignment: organization-defined time period].	Functional	Intersects With	Identifier Management (User Names)	IAC-09	Mechanisms exist to govern naming standards for usernames and Technology Assets, Applications and/or Services (TAAS).	5		Low
IA-04(01)	Identifier Management | Prohibit Account Identifiers as Public Identifiers	Prohibit the use of system account identifiers that are the same as public identifiers for individual accounts.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
IA-04(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
IA-04(03)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
IA-04(04)	Identifier Management | Identify User Status	Manage individual identifiers by uniquely identifying each individual as [Assignment: organization-defined characteristic identifying individual status].	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAC-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	5		Moderate
IA-04(04)	Identifier Management | Identify User Status	Manage individual identifiers by uniquely identifying each individual as [Assignment: organization-defined characteristic identifying individual status].	Functional	Intersects With	User Identity (ID) Management	IAC-09.1	Mechanisms exist to ensure proper user identification management for non-consumer users and administrators.	5		Moderate
IA-04(04)	Identifier Management | Identify User Status	Manage individual identifiers by uniquely identifying each individual as [Assignment: organization-defined characteristic identifying individual status].	Functional	Intersects With	Identity User Status	IAC-09.2	Mechanisms exist to identify contractors and other third-party users through unique username characteristics.	5		Moderate
IA-04(05)	Identifier Management | Dynamic Management	Manage individual identifiers dynamically in accordance with [Assignment: organization-defined dynamic identifier policy].	Functional	Intersects With	Dynamic Management	IAC-09.3	Mechanisms exist to dynamically manage usernames and system identifiers.	5		Not Selected
IA-04(06)	Identifier Management | Cross-organization Management	Coordinate with the following external organizations for cross-organization management of identifiers: [Assignment: organization-defined external organizations].	Functional	Equal	Cross-Organization Management	IAC-09.4	Mechanisms exist to coordinate username identifiers with external organizations for cross-organization management of identifiers.	10		Not Selected
IA-04(07)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
IA-04(08)	Identifier Management | Pairwise Pseudonymous Identifiers	Generate pairwise pseudonymous identifiers.	Functional	Equal	Pairwise Pseudonymous Identifiers (PPID)	IAC-09.6	Mechanisms exist to generate pairwise pseudonymous identifiers with no identifying information about a data subject to discourage activity tracking and profiling of the data subject.	10		Not Selected
IA-04(09)	Management | Attribute Maintenance and	Maintain the attributes for each uniquely identified individual, device, or service in [Assignment: organization-defined protected central storage].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
IA-05	Authenticator Management	Manage system authenticators by:a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator;b. Establishing initial authenticator content for any authenticators issued by the organization;c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators;e. Changing default authenticators prior to first use;f. Changing or refreshing authenticators [Assignment: organization-defined time period by authenticator type] or when [Assignment: organization-defined events] occur;g. Protecting authenticator content from unauthorized disclosure and modification;h. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; andi. Changing authenticators for group or role accounts when membership to those accounts changes.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5		Low

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-53B Baseline
IA-05	Authenticator Management	manage system authenticators by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator;b. Establishing initial authenticator content for any authenticators issued by the organization;c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators;e. Changing default authenticators prior to first use;f. Changing or refreshing authenticators [Assignment: organization-defined time period by authenticator type] or when [Assignment: organization-defined events] occur;g. Protecting authenticator content from unauthorized disclosure and modification;h. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; andi. Changing authenticators for group or role accounts when	Functional	Intersects With	Default Authenticators	IAC-10.8	Mechanisms exist to ensure default authenticators are changed as part of account creation or system installation.	5		Low
IA-05(01)	Authenticator Management | Password-based Authentication	For password-based authentication:a. Maintain a list of commonly-used, expected, or compromised passwords and update the list [Assignment: organization-defined frequency] and when organizational passwords are suspected to have been compromised directly or indirectly;b. Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5(1)(a);c. Transmit passwords only over cryptographically-protected channels;d. Store passwords using an approved salted key derivation function, preferably using a keyed hash;e. Require immediate selection of a new password upon account recovery;f. Allow user selection of long passwords and passphrases, including spaces and all printable characters;g. Employ automated tools to assist the user in selecting strong password authenticators; andh. Enforce the following composition and complexity rules: [Assignment: organization-defined composition and complexity rules].	Functional	Intersects With	Automated Support For Password Strength	IAC-10.4	Automated mechanisms exist to determine if password authenticators are sufficiently strong enough to satisfy organization-defined password length and complexity requirements.	5		Low
IA-05(01)	Authenticator Management | Password-based Authentication	For password-based authentication:a. Maintain a list of commonly-used, expected, or compromised passwords and update the list [Assignment: organization-defined frequency] and when organizational passwords are suspected to have been compromised directly or indirectly;b. Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5(1)(a);c. Transmit passwords only over cryptographically-protected channels;d. Store passwords using an approved salted key derivation function, preferably using a keyed hash;e. Require immediate selection of a new password upon account recovery;f. Allow user selection of long passwords and passphrases, including spaces and all printable characters;g. Employ automated tools to assist the user in selecting strong password authenticators; andh. Enforce the following composition and complexity rules: [Assignment: organization-defined composition and complexity rules].	Functional	Intersects With	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5		Low
IA-05(01)	Authenticator Management | Password-based Authentication	For password-based authentication:a. Maintain a list of commonly-used, expected, or compromised passwords and update the list [Assignment: organization-defined frequency] and when organizational passwords are suspected to have been compromised directly or indirectly;b. Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5(1)(a);c. Transmit passwords only over cryptographically-protected channels;d. Store passwords using an approved salted key derivation function, preferably using a keyed hash;e. Require immediate selection of a new password upon account recovery;f. Allow user selection of long passwords and passphrases, including spaces and all printable characters;g. Employ automated tools to assist the user in selecting strong password authenticators; andh. Enforce the following composition and complexity rules: [Assignment: organization-defined composition and complexity rules].	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5		Low
IA-05(02)	Authenticator Management | Public Key-based Authentication	a. For public key-based authentication:1. Enforce authorized access to the corresponding private key; and2. Map the authenticated identity to the account of the individual or group; andb. When public key infrastructure (PKI) is used:1. Validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information; and2. Implement a local cache of revocation data to support path discovery and validation.	Functional	Equal	PKI-Based Authentication	IAC-10.2	Automated mechanisms exist to validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information for PKI-based authentication.	10		Moderate
IA-05(03)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
IA-05(04)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
IA-05(05)	Authenticator Management | Change Authenticators Prior to Delivery	Require developers and installers of system components to provide unique authenticators or change default authenticators prior to delivery and installation.	Functional	Intersects With	Default Authenticators	IAC-10.8	Mechanisms exist to ensure default authenticators are changed as part of account creation or system installation.	5		Not Selected
IA-05(06)	Authenticator Management | Protection of Authenticators	Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access.	Functional	Intersects With	User Responsibilities for Account Management	IAC-18	Mechanisms exist to compel users to follow accepted practices in the use of authentication mechanisms (e.g., passwords, passphrases, physical or logical security tokens, smart cards, certificates, etc.).	5		Moderate
IA-05(06)	Authenticator Management | Protection of Authenticators	Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access.	Functional	Intersects With	Protection of Authenticators	IAC-10.5	Mechanisms exist to protect authenticators commensurate with the sensitivity of the information to which use of the authenticator permits access.	5		Moderate
IA-05(07)	Authenticator Management | No Embedded Unencrypted Static Authenticators	Ensure that unencrypted static authenticators are not embedded in applications or other forms of static storage.	Functional	Equal	No Embedded Unencrypted Static Authenticators	IAC-10.6	Mechanisms exist to ensure that unencrypted, static authenticators are not embedded in applications, scripts or stored on function keys.	10		Not Selected
IA-05(08)	Authenticator Management | Multiple System Accounts	Implement [Assignment: organization-defined security controls] to manage the risk of compromise due to individuals having accounts on multiple systems.	Functional	Intersects With	Multiple System Accounts	IAC-10.9	Mechanisms exist to implement security safeguards to manage the risk of compromise due to individuals having accounts on multiple Technology Assets, Applications and/or Services (TAAS).	5		Not Selected
IA-05(08)	Authenticator Management | Multiple System Accounts	Implement [Assignment: organization-defined security controls] to manage the risk of compromise due to individuals having accounts on multiple systems.	Functional	Intersects With	Privileged Account Identifiers	IAC-09.5	Mechanisms exist to uniquely manage privileged accounts to identify the account as a privileged user or service.	5		Not Selected
IA-05(09)	Authenticator Management | Federated Credential Management	Use the following external organizations to federate credentials: [Assignment: organization-defined external organizations].	Functional	Equal	Federated Credential Management	IAC-13.2	Mechanisms exist to federate credentials to allow cross-organization authentication of individuals and devices.	10		Not Selected
IA-05(10)	Authenticator Management | Dynamic Credential Binding	Bind identities and authenticators dynamically using the following rules: [Assignment: organization-defined binding rules].	Functional	Intersects With	Dynamic Management	IAC-09.3	Mechanisms exist to dynamically manage usernames and system identifiers.	5		Not Selected
IA-05(11)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
IA-05(12)	Authenticator Management | Biometric Authentication Performance	For biometric-based authentication, employ mechanisms that satisfy the following biometric quality requirements [Assignment: organization-defined biometric quality requirements].	Functional	Equal	Biometric Authentication	IAC-10.12	Mechanisms exist to ensure biometric-based authentication satisfies organization-defined biometric quality requirements for false positives and false negatives.	10		Not Selected

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh	Notes	NIST SP 800-53B Baseline
IA-05(13)	Authenticator Management | Expiration of Cached Authenticators	Prohibit the use of cached authenticators after [Assignment: organization-defined time period].	Functional	Equal	Expiration of Cached Authenticators	IAC-10.10	Automated mechanisms exist to prohibit the use of cached authenticators after organization-defined time period.	10		Not Selected
IA-05(14)	Authenticator Management | Managing Content of PKI Trust Stores	For PKI-based authentication, employ an organization-wide methodology for managing the content of PKI trust stores installed across all platforms, including networks, operating systems, browsers, and applications.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
IA-05(15)	Authenticator Management | GSA-approved Products and Services	Use only General Services Administration-approved products and services for identity, credential, and access management.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
IA-05(16)	Authenticator Management | In-person or Trusted External Party Authenticator Issuance	Require that the issuance of [Assignment: organization-defined types of and/or specific authenticators] be conducted [Selection (one): in person; by a trusted external party] before [Assignment: organization-defined registration authority] with authorization by [Assignment: organization-defined personnel or roles].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
IA-05(17)	Authenticator Management | Presentation Attack Detection for Biometric Authenticators	Employ presentation attack detection mechanisms for biometric-based authentication.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
IA-05(18)	Authenticator Management | Password Managers	a. Employ [Assignment: organization-defined password managers] to generate and manage passwords; andb. Protect the passwords using [Assignment: organization-defined controls].	Functional	Equal	Password Managers	IAC-10.11	Mechanisms exist to protect and store passwords via a password manager tool.	10		Not Selected
IA-06	Authentication Feedback	Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.	Functional	Equal	Authenticator Feedback	IAC-11	Mechanisms exist to obscure the feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	10		Low
IA-07	Cryptographic Module Authentication	Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication.	Functional	Intersects With	Cryptographic Module Authentication	IAC-12	Mechanisms exist to ensure cryptographic modules adhere to applicable statutory, regulatory and contractual requirements for security strength.	5		Low
IA-07	Cryptographic Module Authentication	Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication.	Functional	Intersects With	Automated Authentication Through Cryptographic Modules	CRY-02	Automated mechanisms exist to enable systems to authenticate to a cryptographic module.	5		Low
IA-08	Identification and Authentication (non-organizational Users)	Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.	Functional	Equal	Identification & Authentication for Non-Organizational Users	IAC-03	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) third-party users and processes that provide services to the organization.	10		Low
IA-08(01)	Identification and Authentication (non-organizational Users) | Acceptance of PIV Credentials from Other Agencies	Accept and electronically verify Personal Identity Verification-compliant credentials from other federal agencies.	Functional	Equal	Acceptance of PIV Credentials from Other Organizations	IAC-03.1	Mechanisms exist to accept and electronically verify Personal Identity Verification (PIV) credentials from third-parties.	10		Low
IA-08(02)	Identification and Authentication (non-organizational Users) | Acceptance of External Authenticators	a. Accept only external authenticators that are NIST-compliant; andb. Document and maintain a list of accepted external authenticators.	Functional	Equal	Acceptance of Third-Party Credentials	IAC-03.2	Automated mechanisms exist to accept Federal Identity, Credential and Access Management (FICAM)-approved third-party credentials.	10		Low
IA-08(03)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
IA-08(04)	Identification and Authentication (non-organizational Users) | Use of Defined Profiles	Conform to the following profiles for identity management [Assignment: organization-defined identity management profiles].	Functional	Equal	Use of FICAM-Issued Profiles	IAC-03.3	Mechanisms exist to conform systems to Federal Identity, Credential and Access Management (FICAM)-issued profiles.	10		Low
IA-08(05)	Identification and Authentication (non-organizational Users) | Acceptance of PVI-I Credentials	Accept and verify federated or PKI credentials that meet [Assignment: organization-defined policy].	Functional	Equal	Acceptance of PIV Credentials	IAC-02.3	Mechanisms exist to accept and electronically verify organizational Personal Identity Verification (PIV) credentials.	10		Not Selected
IA-08(06)	Identification and Authentication (non-organizational Users) | Disassociability	Implement the following measures to disassociate user attributes or identifier assertion relationships among individuals, credential service providers, and relying parties: [Assignment: organization-defined measures].	Functional	Equal	Disassociability	IAC-03.4	Mechanisms exist to disassociate user attributes or credential assertion relationships among individuals, credential service providers and relying parties.	10		Not Selected
IA-09	Service Identification and Authentication	Uniquely identify and authenticate [Assignment: organization-defined system services and applications] before establishing communications with devices, users, or other services or applications.	Functional	Equal	Authentication for Third-Party Technology Assets, Applications and/or Services (TAAS)	IAC-05	Mechanisms exist to identify and authenticate third-party Technology Assets, Applications and/or Services (TAAS).	10		Not Selected
IA-09(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
IA-09(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
IA-10	Adaptive Authentication	Require individuals accessing the system to employ [Assignment: organization-defined supplemental authentication techniques or mechanisms] under specific [Assignment: organization-defined circumstances or situations].	Functional	Equal	Adaptive Identification & Authentication	IAC-13	Mechanisms exist to allow individuals to utilize alternative methods of authentication under specific circumstances or situations.	10		Not Selected
IA-11	Re-authentication	Require users to re-authenticate when [Assignment: organization-defined circumstances or situations requiring re-authentication].	Functional	Equal	Re-Authentication	IAC-14	Mechanisms exist to force users and devices to re-authenticate according to organization-defined circumstances that necessitate re-authentication.	10		Low
IA-12	Identity Proofing	a. Identity proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines;b. Resolve user identities to a unique individual; andc. Collect, validate, and verify identity evidence.	Functional	Equal	Identity Proofing (Identity Verification)	IAC-28	Mechanisms exist to verify the identity of a user before issuing authenticators or modifying access permissions.	10		Moderate
IA-12(01)	Identity Proofing | Supervisor Authorization	Require that the registration process to receive an account for logical access includes supervisor or sponsor authorization.	Functional	Intersects With	Management Approval For New or Changed Accounts	IAC-28.1	Mechanisms exist to ensure management approvals are required for new accounts or changes in permissions to existing accounts.	5		Not Selected
IA-12(02)	Identity Proofing | Identity Evidence	Require evidence of individual identification be presented to the registration authority.	Functional	Equal	Identity Evidence	IAC-28.2	Mechanisms exist to require evidence of individual identification to be presented to the registration authority.	10		Moderate
IA-12(03)	Identity Proofing | Identity Evidence Validation and Verification	Require that the presented identity evidence be validated and verified through [Assignment: organizational defined methods of validation and verification].	Functional	Equal	Identity Evidence Validation & Verification	IAC-28.3	Mechanisms exist to require that the presented identity evidence be validated and verified through organizational-defined methods of validation and verification.	10		Moderate
IA-12(04)	Identity Proofing | In-person Validation and Verification	Require that the validation and verification of identity evidence be conducted in person before a designated registration authority.	Functional	Intersects With	User Provisioning & De-Provisioning	IAC-07	Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.	5		High
IA-12(04)	Identity Proofing | In-person Validation and Verification	Require that the validation and verification of identity evidence be conducted in person before a designated registration authority.	Functional	Intersects With	In-Person or Trusted Third-Party Registration	IAC-10.3	Mechanisms exist to conduct in-person or trusted third-party identify verification before user accounts for third-parties are created.	5		High
IA-12(04)	Identity Proofing | In-person Validation and Verification	Require that the validation and verification of identity evidence be conducted in person before a designated registration authority.	Functional	Intersects With	In-Person Validation & Verification	IAC-28.4	Mechanisms exist to require that the validation and verification of identity evidence be conducted in person before a designated registration authority.	5		High
IA-12(05)	Identity Proofing | Address Confirmation	Require that a [Selection (one): registration code; notice of proofing] be delivered through an out-of-band channel to verify the users address (physical or digital) of record.	Functional	Equal	Address Confirmation	IAC-28.5	Mechanisms exist to require that a notice of proofing be delivered through an out-of-band channel to verify the user's address (physical or digital).	10		Moderate
IA-12(06)	Identity Proofing | Accept Externally-proofed Identities	Accept externally-proofed identities at [Assignment: organization-defined identity assurance level].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-53B Baseline
IA-13	Identity Providers and Authorization Servers	Employ identity providers and authorization servers to manage user, device, and non-person entity (NPE) identities, attributes, and access rights supporting authentication and authorization decisions in accordance with [Assignment: organization-defined identification and authentication policy] using [Assignment: organization-defined mechanisms].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
IA-13(01)	Protection of Cryptographic Keys	Cryptographic keys that protect access tokens are generated, managed, and protected from disclosure and misuse.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
IA-13(02)	Verification of Identity and Access Tokens	The source and integrity of identity assertions and access tokens are verified before granting access to system and information resources.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
IA-13(03)	Token Management	In accordance with [Assignment: organization-defined identification and authentication policy], assertions and access tokens are:a. generated;b. issued; c. refreshed;d. revoked;e. time-restricted; andf. audience-restricted.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
IR-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] incident response policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the incident response policy and the associated incident response controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the incident response policy and procedures; andc. Review and update the current incident response:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5		Low
IR-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] incident response policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the incident response policy and the associated incident response controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the incident response policy and procedures; andc. Review and update the current incident response:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Subset Of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	10		Low
IR-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] incident response policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the incident response policy and the associated incident response controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the incident response policy and procedures; andc. Review and update the current incident response:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	IRP Update	IRO-04.2	Mechanisms exist to regularly review and modify incident response practices to incorporate lessons learned, business process changes and industry developments, as necessary.	5		Low
IR-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] incident response policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the incident response policy and the associated incident response controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the incident response policy and procedures; andc. Review and update the current incident response:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	5		Low
IR-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] incident response policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the incident response policy and the associated incident response controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the incident response policy and procedures; andc. Review and update the current incident response:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5		Low
IR-02	Incident Response Training	a. Provide incident response training to system users consistent with assigned roles and responsibilities:1. Within [Assignment: organization-defined time period] of assuming an incident response role or responsibility or acquiring system access;2. When required by system changes; and3. [Assignment: organization-defined frequency] thereafter; andb. Review and update incident response training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Incident Response Training	IRO-05	Mechanisms exist to train personnel in their incident response roles and responsibilities.	5		Low
IR-02(01)	Incident Response Training | Simulated Events	Incorporate simulated events into incident response training to facilitate the required response by personnel in crisis situations.	Functional	Equal	Simulated Incidents	IRO-05.1	Mechanisms exist to incorporate simulated events into incident response training to facilitate effective response by personnel in crisis situations.	10		High
IR-02(02)	Incident Response Training | Automated Training Environments	Provide an incident response training environment using [Assignment: organization-defined automated mechanisms].	Functional	Equal	Automated Incident Response Training Environments	IRO-05.2	Automated mechanisms exist to provide a more thorough and realistic incident response training environment.	10		High
IR-02(03)	Incident Response Training | Breach	Provide incident response training on how to identify and respond to a breach, including the organization's process for reporting a breach.	Functional	Intersects With	Incident Response Training	IRO-05	Mechanisms exist to train personnel in their incident response roles and responsibilities.	5		Not Selected

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh	Notes	NIST SP 800-53B Baseline
IR-03	Incident Response Testing	Test the effectiveness of the incident response capability for the system [Assignment: organization-defined frequency] using the following tests: [Assignment: organization-defined tests].	Functional	Intersects With	Incident Response Testing	IRO-06	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	5		Moderate
IR-03(01)	Incident Response Testing | Automated Testing	Test the incident response capability using [Assignment: organization-defined automated mechanisms].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
IR-03(02)	Incident Response Testing | Coordination with Related Plans	Coordinate incident response testing with organizational elements responsible for related plans.	Functional	Equal	Coordination with Related Plans	IRO-06.1	Mechanisms exist to coordinate incident response testing with organizational elements responsible for related plans.	10		Moderate
IR-03(03)	Incident Response Testing | Continuous Improvement	Use qualitative and quantitative data from testing to:a. Determine the effectiveness of incident response processes;b. Continuously improve incident response processes; andc. Provide incident response measures and metrics that are accurate, consistent, and in a reproducible format.	Functional	Equal	Continuous Incident Response Improvements	IRO-04.3	Mechanisms exist to use qualitative and quantitative data from incident response testing to: (1) Determine the effectiveness of incident response processes; (2) Continuously improve incident response processes; and (3) Provide incident response measures and metrics that are accurate, consistent and in a reproducible format.	10		Not Selected
IR-04	Incident Handling	a. Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery;b. Coordinate incident handling activities with contingency planning activities;c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly; andd. Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.	Functional	Equal	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	10		Low
IR-04(01)	Incident Handling | Automated Incident Handling Processes	Support the incident handling process using [Assignment: organization-defined automated mechanisms].	Functional	Equal	Automated Incident Handling Processes	IRO-02.1	Automated mechanisms exist to support the incident handling process.	10		Moderate
IR-04(02)	Incident Handling | Dynamic Reconfiguration	Include the following types of dynamic reconfiguration for [Assignment: organization-defined system components] as part of the incident response capability: [Assignment: organization-defined types of dynamic reconfiguration].	Functional	Equal	Dynamic Reconfiguration	IRO-02.3	Automated mechanisms exist to dynamically reconfigure system components as part of the incident response capability.	10		Not Selected
IR-04(03)	Incident Handling | Continuity of Operations	Identify [Assignment: organization-defined classes of incidents] and take the following actions in response to those incidents to ensure continuation of organizational mission and business functions: [Assignment: organization-defined actions to take in response to classes of incidents].	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	5		Not Selected
IR-04(03)	Incident Handling | Continuity of Operations	Identify [Assignment: organization-defined classes of incidents] and take the following actions in response to those incidents to ensure continuation of organizational mission and business functions: [Assignment: organization-defined actions to take in response to classes of incidents].	Functional	Intersects With	Incident Classification & Prioritization	IRO-02.4	Mechanisms exist to identify classes of incidents and actions to take to ensure the continuation of organizational missions and business functions.	5		Not Selected
IR-04(04)	Incident Handling | Information Correlation	Correlate incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	5		High
IR-04(04)	Incident Handling | Information Correlation	Correlate incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.	Functional	Intersects With	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.	5		High
IR-04(05)	Incident Handling | Automatic Disabling of System	Implement a configurable capability to automatically disable the system if [Assignment: organization-defined security violations] are detected.	Functional	Intersects With	Automated Response to Suspicious Events	MON-01.11	Automated mechanisms exist to implement pre-determined corrective actions in response to detected events that have security incident implications.	5		Not Selected
IR-04(05)	Incident Handling | Automatic Disabling of System	Implement a configurable capability to automatically disable the system if [Assignment: organization-defined security violations] are detected.	Functional	Intersects With	Automatic Disabling of Technology Assets, Applications and/or Services (TAAS)	IRO-02.6	Mechanisms exist to automatically disable Technology Assets, Applications and/or Services (TAAS), upon detection of a possible incident that meets organizational criteria, which allows for forensic analysis to be performed.	5		Not Selected
IR-04(06)	Incident Handling | Insider Threats	Implement an incident handling capability for incidents involving insider threats.	Functional	Intersects With	Insider Threat Response Capability	IRO-02.2	Mechanisms exist to implement and govern an insider threat program.	5		Not Selected
IR-04(07)	Incident Handling | Insider Threats — Intra-organization Coordination	Coordinate an incident handling capability for insider threats that includes the following organizational entities [Assignment: organization-defined entities].	Functional	Intersects With	Insider Threat Response Capability	IRO-02.2	Mechanisms exist to implement and govern an insider threat program.	5		Not Selected
IR-04(08)	Incident Handling | Correlation with External Organizations	Coordinate with [Assignment: organization-defined external organizations] to correlate and share [Assignment: organization-defined incident information] to achieve a cross-organization perspective on incident awareness and more effective incident responses.	Functional	Equal	Correlation with External Organizations	IRO-02.5	Mechanisms exist to coordinate with approved third-parties to achieve a cross-organization perspective on incident awareness and more effective incident responses.	10		Not Selected
IR-04(09)	Incident Handling | Dynamic Response Capability	Employ [Assignment: organization-defined dynamic response capabilities] to respond to incidents.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
IR-04(10)	Incident Handling | Supply Chain Coordination	Coordinate incident handling activities involving supply chain events with other organizations involved in the supply chain.	Functional	Intersects With	Third-Party Incident Response & Recovery Capabilities	TPM-11	Mechanisms exist to ensure response/recovery planning and testing are conducted with critical suppliers/providers.	5		Not Selected
IR-04(10)	Incident Handling | Supply Chain Coordination	Coordinate incident handling activities involving supply chain events with other organizations involved in the supply chain.	Functional	Intersects With	Supply Chain Coordination	IRO-10.4	Mechanisms exist to provide cybersecurity and data protection incident information to the provider of the Technology Assets, Applications and/or Services (TAAS) and other organizations involved in the supply chain for TAAS related to	5		Not Selected
IR-04(11)	Incident Handling | Integrated Incident Response Team	Establish and maintain an integrated incident response team that can be deployed to any location identified by the organization in [Assignment: organization-defined time period].	Functional	Equal	Integrated Security Incident Response Team (ISIRT)	IRO-07	Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity and data protection incident response operations.	10		High
IR-04(12)	Incident Handling | Malicious Code and Forensic Analysis	Analyze malicious code and/or other residual artifacts remaining in the system after the incident.	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	5		Not Selected
IR-04(12)	Incident Handling | Malicious Code and Forensic Analysis	Analyze malicious code and/or other residual artifacts remaining in the system after the incident.	Functional	Intersects With	Chain of Custody & Forensics	IRO-08	Mechanisms exist to perform digital forensics and maintain the integrity of the chain of custody, in accordance with applicable laws, regulations and industry-recognized secure practices.	5		Not Selected
IR-04(13)	Incident Handling | Behavior Analysis	Analyze anomalous or suspected adversarial behavior in or related to [Assignment: organization-defined environments or resources].	Functional	Intersects With	Honeypots	SEA-11	Mechanisms exist to utilize honeypots that are specifically designed to be the target of malicious attacks for the purpose of detecting, deflecting and analyzing such attacks.	5		Not Selected

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-53B Baseline
IR-04(13)	Incident Handling | Behavior Analysis	Analyze anomalous or suspected adversarial behavior in or related to [Assignment: organization-defined environments or resources].	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	5		Not Selected
IR-04(13)	Incident Handling | Behavior Analysis	Analyze anomalous or suspected adversarial behavior in or related to [Assignment: organization-defined environments or resources].	Functional	Intersects With	Honeyclients	SEA-12	Mechanisms exist to utilize honeyclients that proactively seek to identify malicious websites and/or web-based malicious code.	5		Not Selected
IR-04(14)	Incident Handling | Security Operations Center	Establish and maintain a security operations center.	Functional	Equal	Security Operations Center (SOC)	OPS-04	Mechanisms exist to establish and maintain a Security Operations Center (SOC) that facilitates a 24x7 response capability.	10		Not Selected
IR-04(15)	Incident Handling | Public Relations and Reputation Repair	a. Manage public relations associated with an incident; andb. Employ measures to repair the reputation of the organization.	Functional	Equal	Public Relations & Reputation Repair	IRO-16	Mechanisms exist to proactively manage public relations associated with incidents and employ appropriate measures to prevent further reputational damage and develop plans to repair any damage to the organization's reputation.	10		Not Selected
IR-05	Incident Monitoring	Track and document incidents.	Functional	Equal	Situational Awareness For Incidents	IRO-09	Mechanisms exist to document, monitor and report the status of cybersecurity and data protection incidents to internal stakeholders all the way through the resolution of the incident.	10		Low
IR-05(01)	Incident Monitoring | Automated Tracking, Data Collection, and Analysis	Track incidents and collect and analyze incident information using [Assignment: organization-defined automated mechanisms].	Functional	Equal	Automated Tracking, Data Collection & Analysis	IRO-09.1	Automated mechanisms exist to assist in the tracking, collection and analysis of information from actual and potential cybersecurity and data protection incidents.	10		High
IR-06	Incident Reporting	a. Require personnel to report suspected incidents to the organizational incident response capability within [Assignment: organization-defined time period]; andb. Report incident information to [Assignment: organization-defined authorities].	Functional	Intersects With	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5		Low
IR-06	Incident Reporting	a. Require personnel to report suspected incidents to the organizational incident response capability within [Assignment: organization-defined time period]; andb. Report incident information to [Assignment: organization-defined authorities].	Functional	Intersects With	Regulatory & Law Enforcement Contacts	IRO-14	Mechanisms exist to maintain incident response contacts with applicable regulatory and law enforcement agencies.	5		Low
IR-06	Incident Reporting	a. Require personnel to report suspected incidents to the organizational incident response capability within [Assignment: organization-defined time period]; andb. Report incident information to [Assignment: organization-defined authorities].	Functional	Intersects With	Contacts With Authorities	GOV-06	Mechanisms exist to identify and document appropriate contacts with relevant law enforcement and regulatory bodies.	5		Low
IR-06(01)	Incident Reporting | Automated Reporting	Report incidents using [Assignment: organization-defined automated mechanisms].	Functional	Equal	Automated Reporting	IRO-10.1	Automated mechanisms exist to assist in the reporting of cybersecurity and data protection incidents.	10		Moderate
IR-06(02)	Incident Reporting | Vulnerabilities Related to Incidents	Report system vulnerabilities associated with reported incidents to [Assignment: organization-defined personnel or roles].	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	5		Not Selected
IR-06(02)	Incident Reporting | Vulnerabilities Related to Incidents	Report system vulnerabilities associated with reported incidents to [Assignment: organization-defined personnel or roles].	Functional	Intersects With	Vulnerabilities Related To Incidents	IRO-10.3	Mechanisms exist to report system vulnerabilities associated with reported cybersecurity and data protection incidents to organization-defined personnel or roles.	5		Not Selected
IR-06(03)	Incident Reporting | Supply Chain Coordination	Provide incident information to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident.	Functional	Intersects With	Supply Chain Coordination	IRO-10.4	Mechanisms exist to provide cybersecurity and data protection incident information to the provider of the Technology Assets, Applications and/or Services (TAAS) and other organizations involved in the supply chain for TAAS related to	5		Moderate
IR-07	Incident Response Assistance	Provide an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the system for the handling and reporting of incidents.	Functional	Equal	Incident Reporting Assistance	IRO-11	Mechanisms exist to provide incident response advice and assistance to users of Technology Assets, Applications and/or Services (TAAS) for the handling and reporting of actual and potential cybersecurity and data protection incidents.	10		Low
IR-07(01)	Incident Response Assistance | Automation Support for Availability of Information and Support	Increase the availability of incident response information and support using [Assignment: organization-defined automated mechanisms].	Functional	Equal	Automation Support of Availability of Information / Support	IRO-11.1	Automated mechanisms exist to increase the availability of incident response-related information and support.	10		Moderate
IR-07(02)	Incident Response Assistance | Coordination with External Providers	a. Establish a direct, cooperative relationship between its incident response capability and external providers of system protection capability; andb. Identify organizational incident response team members to the external providers.	Functional	Equal	Coordination With External Providers	IRO-11.2	Mechanisms exist to establish a direct, cooperative relationship between the organization's incident response capability and external service providers.	10		Not Selected
IR-08	Incident Response Plan	a. Develop an incident response plan that:1. Provides the organization with a roadmap for implementing its incident response capability;2. Describes the structure and organization of the incident response capability;3. Provides a high-level approach for how the incident response capability fits into the overall organization;4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;5. Defines reportable incidents;6. Provides metrics for measuring the incident response capability within the organization;7. Defines the resources and management support needed to effectively maintain and mature an incident response capability;8. Addresses the sharing of incident information;9. Is reviewed and approved by [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency]; and10. Explicitly designates responsibility for incident response to [Assignment: organization-defined entities, personnel, or roles].b. Distribute copies of the incident response plan to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements];c. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing;d. Communicate incident response plan changes to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; ande. Protect the incident response plan from unauthorized disclosure and modification.	Functional	Equal	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	10		Low
IR-08(01)	Incident Response Plan | Breaches	Include the following in the Incident Response Plan for breaches involving personally identifiable information:a. A process to determine if notice to individuals or other organizations, including oversight organizations, is needed;b. An assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms; andc. Identification of applicable privacy requirements.	Functional	Equal	Data Breach	IRO-04.1	Mechanisms exist to address data breaches, or other incidents involving the unauthorized disclosure of sensitive or regulated data, according to applicable laws, regulations and contractual obligations.	10		Not Selected

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-53B Baseline
IR-09	Information Spillage Response	Respond to information spills by:a. Assigning [Assignment: organization-defined personnel or roles] with responsibility for responding to information spills;b. Identifying the specific information involved in the system contamination;c. Alerting [Assignment: organization-defined personnel or roles] of the information spill using a method of communication not associated with the spill;d. Isolating the contaminated system or system component;e. Eradicating the information from the contaminated system or component;f. Identifying other systems or system components that may have been subsequently contaminated; andg. Performing the following additional actions: [Assignment: organization-defined actions].	Functional	Intersects With	Sensitive / Regulated Data Spill Response	IRO-12	Mechanisms exist to respond to sensitive/regulated data spills.	5		Not Selected
IR-09	Information Spillage Response	Respond to information spills by:a. Assigning [Assignment: organization-defined personnel or roles] with responsibility for responding to information spills;b. Identifying the specific information involved in the system contamination;c. Alerting [Assignment: organization-defined personnel or roles] of the information spill using a method of communication not associated with the spill;d. Isolating the contaminated system or system component;e. Eradicating the information from the contaminated system or component;f. Identifying other systems or system components that may have been subsequently contaminated; andg. Performing the following additional actions: [Assignment: organization-defined actions].	Functional	Intersects With	Sensitive / Regulated Data Spill Responsible Personnel	IRO-12.1	Mechanisms exist to formally assign personnel or roles with responsibility for responding to sensitive/regulated data spills.	5		Not Selected
IR-09(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
IR-09(02)	Information Spillage Response | Training	Provide information spillage response training [Assignment: organization-defined frequency].	Functional	Equal	Sensitive / Regulated Data Spill Training	IRO-12.2	Mechanisms exist to ensure incident response training material provides coverage for sensitive/regulated data spillage response.	10		Not Selected
IR-09(03)	Information Spillage Response | Post-spill Operations	Implement the following procedures to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions: [Assignment: organization-defined procedures].	Functional	Equal	Post-Sensitive / Regulated Data Spill Operations	IRO-12.3	Mechanisms exist to ensure that organizational personnel impacted by sensitive/regulated data spills can continue to carry out assigned tasks while contaminated Technology Assets, Applications and/or Services (TAAS) are undergoing	10		Not Selected
IR-09(04)	Information Spillage Response | Exposure to Unauthorized Personnel	Employ the following controls for personnel exposed to information not within assigned access authorizations: [Assignment: organization-defined controls].	Functional	Equal	Sensitive / Regulated Data Exposure to Unauthorized Personnel	IRO-12.4	Mechanisms exist to address security safeguards for personnel exposed to sensitive/regulated data that is not within their assigned access authorizations.	10		Not Selected
IR-10		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
MA-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] maintenance policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the maintenance policy and the associated maintenance controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the maintenance policy and procedures; andc. Review and update the current maintenance:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Subset Of	Maintenance Operations	MNT-01	Mechanisms exist to develop, disseminate, review & update procedures to facilitate the implementation of maintenance controls across the enterprise.	10		Low
MA-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] maintenance policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the maintenance policy and the associated maintenance controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the maintenance policy and procedures; andc. Review and update the current maintenance:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Remote Maintenance Notifications	MNT-05.2	Mechanisms exist to require maintenance personnel to notify affected stakeholders when remote, non-local maintenance is planned (e.g., date/time).	5		Low
MA-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] maintenance policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the maintenance policy and the associated maintenance controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the maintenance policy and procedures; andc. Review and update the current maintenance:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Auditing Remote Maintenance	MNT-05.1	Mechanisms exist to audit remote, non-local maintenance and diagnostic sessions, as well as review the maintenance action performed during remote maintenance sessions.	5		Low
MA-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] maintenance policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the maintenance policy and the associated maintenance controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the maintenance policy and procedures; andc. Review and update the current maintenance:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5		Low

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-53B Baseline
MA-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] maintenance policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the maintenance policy and the associated maintenance controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the maintenance policy and procedures; andc. Review and update the current maintenance:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5		Low
MA-02	Controlled Maintenance	maintenance, repair, and replacement on system components in accordance with manufacturer or vendor specifications and/or organizational requirements;b. Approve and monitor all maintenance activities, whether performed on site or remotely and whether the system or system components are serviced on site or removed to another location;c. Require that [Assignment: organization-defined personnel or roles] explicitly approve the removal of the system or system components from organizational facilities for off-site maintenance, repair, or replacement;d. Sanitize equipment to remove the following information from associated media prior to removal from organizational facilities for off-site maintenance, repair, or replacement: [Assignment: organization-defined information];e. Check all potentially impacted controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions; andf. Include the following information in organizational maintenance records: [Assignment: organization-defined	Functional	Equal	Controlled Maintenance	MNT-02	Mechanisms exist to conduct controlled maintenance activities throughout the lifecycle of the Technology Asset, Application and/or Service (TAAS).	10		Low
MA-02(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
MA-02(02)	Controlled Maintenance | Automated Maintenance Activities	a. Schedule, conduct, and document maintenance, repair, and replacement actions for the system using [Assignment: organization-defined automated mechanisms]; andb. Produce up-to date, accurate, and complete records of all maintenance, repair, and replacement actions requested, scheduled, in process, and completed.	Functional	Equal	Automated Maintenance Activities	MNT-02.1	Automated mechanisms exist to schedule, conduct and document maintenance and repairs.	10		High
MA-03	Maintenance Tools	a. Approve, control, and monitor the use of system maintenance tools; andb. Review previously approved system maintenance tools [Assignment: organization-defined frequency].	Functional	Intersects With	Maintenance Tools	MNT-04	Mechanisms exist to control and monitor the use of system maintenance tools.	5		Moderate
MA-03(01)	Maintenance Tools | Inspect Tools	Inspect the maintenance tools used by maintenance personnel for improper or unauthorized modifications.	Functional	Equal	Inspect Tools	MNT-04.1	Mechanisms exist to inspect maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.	10		Moderate
MA-03(02)	Maintenance Tools | Inspect Media	Check media containing diagnostic and test programs for malicious code before the media are used in the system.	Functional	Equal	Inspect Media	MNT-04.2	Mechanisms exist to check media containing diagnostic and test programs for malicious code before the media are used.	10		Moderate
MA-03(03)	Maintenance Tools | Prevent Unauthorized Removal	Prevent the removal of maintenance equipment containing organizational information by:a. Verifying that there is no organizational information contained on the equipment;b. Sanitizing or destroying the equipment;c. Retaining the equipment within the facility; ord. Obtaining an exemption from [Assignment: organization-defined personnel or roles] explicitly authorizing removal of the equipment from the facility.	Functional	Equal	Prevent Unauthorized Removal	MNT-04.3	Mechanisms exist to prevent or control the removal of equipment undergoing maintenance that contains organizational information.	10		Moderate
MA-03(04)	Maintenance Tools | Restricted Tool Use	Restrict the use of maintenance tools to authorized personnel only.	Functional	Equal	Restrict Tool Usage	MNT-04.4	Automated mechanisms exist to restrict the use of maintenance tools to authorized maintenance personnel and/or roles.	10		Not Selected
MA-03(05)	Maintenance Tools | Execution with Privilege	Monitor the use of maintenance tools that execute with increased privilege.	Functional	Intersects With	Maintenance Tools	MNT-04	Mechanisms exist to control and monitor the use of system maintenance tools.	5		Not Selected
MA-03(06)	Maintenance Tools | Software Updates and Patches	Inspect maintenance tools to ensure the latest software updates and patches are installed.	Functional	Intersects With	Maintenance Tools	MNT-04	Mechanisms exist to control and monitor the use of system maintenance tools.	5		Not Selected
MA-04	Nonlocal Maintenance	a. Approve and monitor nonlocal maintenance and diagnostic activities;b. Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system;c. Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions;d. Maintain records for nonlocal maintenance and diagnostic activities; ande. Terminate session and network connections when nonlocal maintenance is completed	Functional	Intersects With	Remote Maintenance	MNT-05	Mechanisms exist to authorize, monitor and control remote, non-local maintenance and diagnostic activities.	5		Low
MA-04	Nonlocal Maintenance	a. Approve and monitor nonlocal maintenance and diagnostic activities;b. Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system;c. Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions;d. Maintain records for nonlocal maintenance and diagnostic activities; ande. Terminate session and network connections when nonlocal maintenance is completed	Functional	Intersects With	Remote Maintenance Notifications	MNT-05.2	Mechanisms exist to require maintenance personnel to notify affected stakeholders when remote, non-local maintenance is planned (e.g., date/time).	5		Low
MA-04	Nonlocal Maintenance	a. Approve and monitor nonlocal maintenance and diagnostic activities;b. Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system;c. Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions;d. Maintain records for nonlocal maintenance and diagnostic activities; ande. Terminate session and network connections when nonlocal maintenance is completed	Functional	Intersects With	Auditing Remote Maintenance	MNT-05.1	Mechanisms exist to audit remote, non-local maintenance and diagnostic sessions, as well as review the maintenance action performed during remote maintenance sessions.	5		Low
MA-04(01)	Nonlocal Maintenance | Logging and Review	a. Log [Assignment: organization-defined audit events] for nonlocal maintenance and diagnostic sessions; andb. Review the audit records of the maintenance and diagnostic sessions to detect anomalous behavior.	Functional	Intersects With	Auditing Remote Maintenance	MNT-05.1	Mechanisms exist to audit remote, non-local maintenance and diagnostic sessions, as well as review the maintenance action performed during remote maintenance sessions.	5		Not Selected
MA-04(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
MA-04(03)	Nonlocal Maintenance | Comparable Security and Sanitization	a. Require that nonlocal maintenance and diagnostic services be performed from a system that implements a security capability comparable to the capability implemented on the system being serviced; orb. Remove the component to be serviced from the system prior to nonlocal maintenance or diagnostic services; sanitize the component (for organizational information); and after the service is performed, inspect and sanitize the component (for potentially malicious software) before reconnecting the component to the system.	Functional	Equal	Remote Maintenance Comparable Security & Sanitization	MNT-05.6	Mechanisms exist to require Technology Assets, Applications and/or Services (TAAS) performing remote, non-local maintenance and/or diagnostic services implement a security capability comparable to the capability implemented on the system being serviced.	10		High
MA-04(04)	Nonlocal Maintenance | Authentication and Separation of Maintenance Sessions	Protect nonlocal maintenance sessions by:a. Employing [Assignment: organization-defined authenticators that are replay resistant]; andb. Separating the maintenance sessions from other network sessions with the system by either:1. Physically separated communications paths; or2. Logically separated communications paths.	Functional	Equal	Separation of Maintenance Sessions	MNT-05.7	Mechanisms exist to protect maintenance sessions through replay-resistant sessions that are physically or logically separated communications paths from other network sessions.	10		Not Selected
MA-04(05)	Nonlocal Maintenance | Approvals and Notifications	a. Require the approval of each nonlocal maintenance session by [Assignment: organization-defined personnel or roles]; andb. Notify the following personnel or roles of the date and time of planned nonlocal maintenance: [Assignment: organization-defined personnel or roles].	Functional	Equal	Remote Maintenance Pre-Approval	MNT-05.5	Mechanisms exist to require maintenance personnel to obtain pre-approval and scheduling for remote, non-local maintenance sessions.	10		Not Selected

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh	Notes	NIST SP 800-53B Baseline
MA-04(06)	Nonlocal Maintenance | Cryptographic Protection	Implement the following cryptographic mechanisms to protect the integrity and confidentiality of nonlocal maintenance and diagnostic communications: [Assignment: organization-defined cryptographic mechanisms].	Functional	Equal	Remote Maintenance Cryptographic Protection	MNT-05.3	Cryptographic mechanisms exist to protect the integrity and confidentiality of remote, non-local maintenance and diagnostic communications.	10		Not Selected
MA-04(07)	Nonlocal Maintenance | Disconnect Verification	Verify session and network connection termination after the completion of nonlocal maintenance and diagnostic sessions.	Functional	Equal	Remote Maintenance Disconnect Verification	MNT-05.4	Mechanisms exist to provide remote disconnect verification to ensure remote, non-local maintenance and diagnostic sessions are properly terminated.	10		Not Selected
MA-05	Maintenance Personnel	a. Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel;b. Verify that non-escorted personnel performing maintenance on the system possess the required access authorizations; andc. Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.	Functional	Equal	Authorized Maintenance Personnel	MNT-06	Mechanisms exist to maintain a current list of authorized maintenance organizations or personnel.	10		Low
MA-05(01)	Maintenance Personnel | Individuals Without Appropriate Access	a. Implement procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements:1. Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified; and2. Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; andb. Develop and implement [Assignment: organization-defined alternate controls] in the event a system component cannot be sanitized, removed, or disconnected from the system.	Functional	Intersects With	Maintenance Personnel Without Appropriate Access	MNT-06.1	Mechanisms exist to ensure the risks associated with maintenance personnel who do not have appropriate access authorizations, clearances or formal access approvals are appropriately mitigated.	5		High
MA-05(02)	Maintenance Personnel | Security Clearances for Classified Systems	Verify that personnel performing maintenance and diagnostic activities on a system processing, storing, or transmitting classified information possess security clearances and formal access approvals for at least the highest classification level and for compartments of information on the system.	Functional	Intersects With	Maintenance Personnel Without Appropriate Access	MNT-06.1	Mechanisms exist to ensure the risks associated with maintenance personnel who do not have appropriate access authorizations, clearances or formal access approvals are appropriately mitigated.	5		Not Selected
MA-05(03)	Maintenance Personnel | Citizenship Requirements for Classified Systems	Verify that personnel performing maintenance and diagnostic activities on a system processing, storing, or transmitting classified information are U.S. citizens.	Functional	Intersects With	Maintenance Personnel Without Appropriate Access	MNT-06.1	Mechanisms exist to ensure the risks associated with maintenance personnel who do not have appropriate access authorizations, clearances or formal access approvals are appropriately mitigated.	5		Not Selected
MA-05(04)	Maintenance Personnel | Foreign Nationals	Ensure that:a. Foreign nationals with appropriate security clearances are used to conduct maintenance and diagnostic activities on classified systems only when the systems are jointly owned and operated by the United States and foreign allied governments, or owned and operated solely by foreign allied governments; andb. Approvals, consents, and detailed operational conditions regarding the use of foreign nationals to conduct maintenance and diagnostic activities on classified systems are fully documented within Memoranda of Agreements.	Functional	Intersects With	Maintenance Personnel Without Appropriate Access	MNT-06.1	Mechanisms exist to ensure the risks associated with maintenance personnel who do not have appropriate access authorizations, clearances or formal access approvals are appropriately mitigated.	5		Not Selected
MA-05(05)	Maintenance Personnel | Non-system Maintenance	Ensure that non-escorted personnel performing maintenance activities not directly associated with the system but in the physical proximity of the system, have required access authorizations.	Functional	Equal	Non-System Related Maintenance	MNT-06.2	Mechanisms exist to ensure that non-escorted personnel performing non-IT maintenance activities in the physical proximity of systems have required access authorizations.	10		Not Selected
MA-06	Timely Maintenance	Obtain maintenance support and/or spare parts for [Assignment: organization-defined system components] within [Assignment: organization-defined time period] of failure.	Functional	Equal	Timely Maintenance	MNT-03	Mechanisms exist to obtain maintenance support and/or spare parts for Technology Assets, Applications and/or Services (TAAS) within a defined Recovery Time Objective (RTO).	10		Moderate
MA-06(01)	Timely Maintenance | Preventive Maintenance	Perform preventive maintenance on [Assignment: organization-defined system components] at [Assignment: organization-defined time intervals].	Functional	Equal	Preventative Maintenance	MNT-03.1	Mechanisms exist to perform preventive maintenance on critical Technology Assets, Applications and/or Services (TAAS).	10		Not Selected
MA-06(02)	Timely Maintenance | Predictive Maintenance	Perform predictive maintenance on [Assignment: organization-defined system components] at [Assignment: organization-defined time intervals].	Functional	Equal	Predictive Maintenance	MNT-03.2	Mechanisms exist to perform predictive maintenance on critical Technology Assets, Applications and/or Services (TAAS).	10		Not Selected
MA-06(03)	Timely Maintenance | Automated Support for Predictive Maintenance	Transfer predictive maintenance data to a maintenance management system using [Assignment: organization-defined automated mechanisms].	Functional	Equal	Automated Support For Predictive Maintenance	MNT-03.3	Automated mechanisms exist to transfer predictive maintenance data to a computerized maintenance management system.	10		Not Selected
MA-07	Field Maintenance	Restrict or prohibit field maintenance on [Assignment: organization-defined systems or system components] to [Assignment: organization-defined trusted maintenance facilities].	Functional	Equal	Field Maintenance	MNT-08	Mechanisms exist to securely conduct field maintenance on geographically deployed assets.	10		Not Selected
MP-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] media protection policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the media protection policy and the associated media protection controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the media protection policy and procedures; andc. Review and update the current media protection:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5		Low
MP-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] media protection policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the media protection policy and the associated media protection controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the media protection policy and procedures; andc. Review and update the current media protection:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10		Low

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh	Notes	NIST SP 800-53B Baseline
MP-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] media protection policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the media protection policy and the associated media protection controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the media protection policy and procedures; andc. Review and update the current media protection:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5		Low
MP-02	Media Access	Restrict access to [Assignment: organization-defined types of digital and/or non-digital media] to [Assignment: organization-defined personnel or roles].	Functional	Intersects With	Media Access	DCH-03	Mechanisms exist to control and restrict access to digital and non-digital media to authorized individuals.	5		Low
MP-02	Media Access	Restrict access to [Assignment: organization-defined types of digital and/or non-digital media] to [Assignment: organization-defined personnel or roles].	Functional	Intersects With	Endpoint Device Management (EDM)	END-01	Mechanisms exist to facilitate the implementation of Endpoint Device Management (EDM) controls.	5		Low
MP-02(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
MP-02(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
MP-03	Media Marking	a. Mark system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; andb. Exempt [Assignment: organization-defined types of system media] from marking if the media remain within [Assignment: organization-defined controlled areas].	Functional	Intersects With	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	5		Moderate
MP-03	Media Marking	a. Mark system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; andb. Exempt [Assignment: organization-defined types of system media] from marking if the media remain within [Assignment: organization-defined controlled areas].	Functional	Intersects With	Automated Marking	DCH-04.1	Automated mechanisms exist to mark physical media and digital files to indicate the distribution limitations, handling requirements and applicable security markings (if any) of the information to aid Data Loss Prevention (DLP) technologies.	5		Moderate
MP-04	Media Storage	a. Physically control and securely store [Assignment: organization-defined types of digital and/or non-digital media] within [Assignment: organization-defined controlled areas]; andb. Protect system media types defined in MP-4a until the media are destroyed or sanitized using approved equipment, techniques, and procedures.	Functional	Equal	Media Storage	DCH-06	Mechanisms exist to: (1) Physically control and securely store digital and non-digital media within controlled areas using organization-defined security measures; and (2) Protect system media until the media are destroyed or sanitized using approved equipment, techniques and procedures.	10		Moderate
MP-04(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
MP-04(02)	Media Storage | Automated Restricted Access	Restrict access to media storage areas and log access attempts and access granted using [Assignment: organization-defined automated mechanisms].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
MP-05	Media Transport	a. Protect and control [Assignment: organization-defined types of system media] during transport outside of controlled areas using [Assignment: organization-defined controls];b. Maintain accountability for system media during transport outside of controlled areas;c. Document activities associated with the transport of system media; andd. Restrict the activities associated with the transport of system media to authorized personnel.	Functional	Equal	Media Transportation	DCH-07	Mechanisms exist to protect and control digital and non-digital media during transport outside of controlled areas using appropriate security measures.	10		Moderate
MP-05(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
MP-05(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
MP-05(03)	Media Transport | Custodians	Employ an identified custodian during transport of system media outside of controlled areas.	Functional	Equal	Custodians	DCH-07.1	Mechanisms exist to identify custodians throughout the transport of digital or non-digital media.	10		Not Selected
MP-05(04)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
MP-06	Media Sanitization	a. Sanitize [Assignment: organization-defined system media] prior to disposal, release out of organizational control, or release for reuse using [Assignment: organization-defined sanitization techniques and procedures]; andb. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.	Functional	Intersects With	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	5		Low
MP-06	Media Sanitization	a. Sanitize [Assignment: organization-defined system media] prior to disposal, release out of organizational control, or release for reuse using [Assignment: organization-defined sanitization techniques and procedures]; andb. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.	Functional	Intersects With	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5		Low
MP-06	Media Sanitization	a. Sanitize [Assignment: organization-defined system media] prior to disposal, release out of organizational control, or release for reuse using [Assignment: organization-defined sanitization techniques and procedures]; andb. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.	Functional	Intersects With	Sanitization of Personal Data (PD)	DCH-09.3	Mechanisms exist to facilitate the sanitization of Personal Data (PD).	5		Low
MP-06(01)	Media Sanitization | Review, Approve, Track, Document, and Verify	Review, approve, track, document, and verify media sanitization and disposal actions.	Functional	Equal	System Media Sanitization Documentation	DCH-09.1	Mechanisms exist to supervise, track, document and verify system media sanitization and disposal actions.	10		High
MP-06(02)	Media Sanitization | Equipment Testing	Test sanitization equipment and procedures [Assignment: organization-defined frequency] to ensure that the intended sanitization is being achieved.	Functional	Equal	Equipment Testing	DCH-09.2	Mechanisms exist to test sanitization equipment and procedures to verify that the intended result is achieved.	10		High
MP-06(03)	Media Sanitization | Nondestructive Techniques	Apply nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the system under the following circumstances: [Assignment: organization-defined circumstances requiring sanitization of portable	Functional	Intersects With	First Time Use Sanitization	DCH-09.4	Mechanisms exist to apply nondestructive sanitization techniques to portable storage devices prior to first use.	5		High
MP-06(03)	Media Sanitization | Nondestructive Techniques	Apply nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the system under the following circumstances: [Assignment: organization-defined circumstances requiring sanitization of portable storage devices].	Functional	Intersects With	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5		High
MP-06(03)	Media Sanitization | Nondestructive Techniques	Apply nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the system under the following circumstances: [Assignment: organization-defined circumstances requiring sanitization of portable	Functional	Intersects With	Sanitization of Personal Data (PD)	DCH-09.3	Mechanisms exist to facilitate the sanitization of Personal Data (PD).	5		High
MP-06(04)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
MP-06(05)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
MP-06(06)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
MP-06(07)	Media Sanitization | Dual Authorization	Enforce dual authorization for the sanitization of [Assignment: organization-defined system media].	Functional	Equal	Dual Authorization for Sensitive Data Destruction	DCH-09.5	Mechanisms exist to enforce dual authorization for the destruction, disposal or sanitization of digital media that contains sensitive/regulated data.	10		Not Selected
MP-06(08)	Media Sanitization | Remote Purging or Wiping of Information	Provide the capability to purge or wipe information from [Assignment: organization-defined systems or system components] [Selection (one): remotely; under the following conditions: [Assignment: organization-defined conditions]].	Functional	Equal	Remote Purging	MDM-05	Mechanisms exist to remotely purge selected information from mobile devices.	10		Not Selected

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-53B Baseline
MP-07	Media Use	a. [Selection (one): Restrict; Prohibit] the use of [Assignment: organization-defined types of system media] on [Assignment: organization-defined systems or system components] using [Assignment: organization-defined controls]; andb. Prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner.	Functional	Intersects With	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	5		Low
MP-07	Media Use	a. [Selection (one): Restrict; Prohibit] the use of [Assignment: organization-defined types of system media] on [Assignment: organization-defined systems or system components] using [Assignment: organization-defined controls]; andb. Prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner.	Functional	Intersects With	Media Use	DCH-10	Mechanisms exist to restrict the use of types of digital media on systems or system components.	5		Low
MP-07	Media Use	a. [Selection (one): Restrict; Prohibit] the use of [Assignment: organization-defined types of system media] on [Assignment: organization-defined systems or system components] using [Assignment: organization-defined controls]; andb. Prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner.	Functional	Intersects With	Prohibit Use Without Owner	DCH-10.2	Mechanisms exist to prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner.	5		Low
MP-07(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
MP-07(02)	Media Use | Prohibit Use of Sanitization-resistant Media	Prohibit the use of sanitization-resistant media in organizational systems.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
MP-08	Media Downgrading	a. Establish [Assignment: organization-defined system media downgrading process] that includes employing downgrading mechanisms with strength and integrity commensurate with the security category or classification of the information;b. Verify that the 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. Identify [Assignment: organization-defined system media requiring downgrading]; andd. Downgrade the identified system media using the established process.	Functional	Intersects With	Data Reclassification	DCH-11	Mechanisms exist to reclassify data, including associated Technology Assets, Applications and/or Services (TAAS), commensurate with the security category and/or classification level of the information.	5		Not Selected
MP-08(01)	Media Downgrading | Documentation of Process	Document system media downgrading actions.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
MP-08(02)	Media Downgrading | Equipment Testing	Test downgrading equipment and procedures [Assignment: organization-defined frequency] to ensure that downgrading actions are being achieved.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
MP-08(03)	Media Downgrading | Controlled Unclassified Information	Downgrade system media containing controlled unclassified information prior to public release.	Functional	Intersects With	Data Reclassification	DCH-11	Mechanisms exist to reclassify data, including associated Technology Assets, Applications and/or Services (TAAS), commensurate with the security category and/or classification level of the information.	5		Not Selected
MP-08(04)	Media Downgrading | Classified Information	Downgrade system media containing classified information prior to release to individuals without required access authorizations.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
PE-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] physical and environmental protection policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the physical and environmental protection policy and the associated physical and environmental protection controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures; andc. Review and update the current physical and environmental protection:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5		Low
PE-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] physical and environmental protection policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the physical and environmental protection policy and the associated physical and environmental protection controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures; andc. Review and update the current physical and environmental protection:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10		Low
PE-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] physical and environmental protection policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the physical and environmental protection policy and the associated physical and environmental protection controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures; andc. Review and update the current physical and environmental protection:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5		Low
PE-02	Physical Access Authorizations	a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides;b. Issue authorization credentials for facility access;c. Review the access list detailing authorized facility access by individuals [Assignment: organization-defined frequency]; andd. Remove individuals from the facility access list when access is no longer required.	Functional	Equal	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	10		Low
PE-02(01)	Physical Access Authorizations | Access by Position or Role	Authorize physical access to the facility where the system resides based on position or role.	Functional	Equal	Role-Based Physical Access	PES-02.1	Physical access control mechanisms exist to authorize physical access to facilities based on the position or role of the individual.	10		Not Selected
PE-02(02)	Physical Access Authorizations | Two Forms of Identification	Require two forms of identification from the following forms of identification for visitor access to the facility where the system resides: [Assignment: organization-defined list of acceptable forms of identification].	Functional	Equal	Identification Requirement	PES-06.2	Physical access control mechanisms exist to requires at least one(1) form of government-issued or organization-issued photo identification to authenticate individuals before they can gain access to the facility.	10		Not Selected

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-53B Baseline
PE-02(03)	Physical Access Authorizations | Restrict Unescorted Access	Restrict unescorted access to the facility where the system resides to personnel with [Selection (one or more): security clearances for all information contained within the system; formal access authorizations for all information contained within the system; need for access to all information contained within the system; [Assignment: organization-defined physical access authorizations]].	Functional	Equal	Restrict Unescorted Access	PES-06.3	Physical access control mechanisms exist to restrict unescorted access to facilities to personnel with required security clearances, formal access authorizations and validate the need for access.	10		Not Selected
PE-03	Physical Access Control	[Assignment: organization-defined entry and exit points to the facility where the system resides] by:1. Verifying individual access authorizations before granting access to the facility; and2. Controlling ingress and egress to the facility using [Selection (one or more): [Assignment: organization-defined physical access control systems or devices]; guards];b. Maintain physical access audit logs for [Assignment: organization-defined entry or exit points];c. Control access to areas within the facility designated as publicly accessible by implementing the following controls: [Assignment: organization-defined physical access controls];d. Escort visitors and control visitor activity [Assignment: organization-defined circumstances requiring visitor escorts and control of visitor activity];e. Secure keys, combinations, and other physical access devices;f. Inventory [Assignment: organization-defined physical access devices] every [Assignment: organization-defined frequency]; andg. Change combinations and keys [Assignment: organization-defined frequency] and/or when keys are lost, combinations are compromised, or when individuals possessing the keys or combinations	Functional	Intersects With	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	5		Low
PE-03(01)	Physical Access Control | System Access	Enforce physical access authorizations to the system in addition to the physical access controls for the facility at [Assignment: organization-defined physical spaces containing one or more components of the system].	Functional	Equal	Access To Critical Systems	PES-03.4	Physical access control mechanisms exist to enforce physical access to critical systems or sensitive/regulated data, in addition to the physical access controls for the facility.	10		High
PE-03(02)	Physical Access Control | Facility and Systems	Perform security checks [Assignment: organization-defined frequency] at the physical perimeter of the facility or system for exfiltration of information or removal of system components.	Functional	Intersects With	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	5		Not Selected
PE-03(03)	Physical Access Control | Continuous Guards	Employ guards to control [Assignment: organization-defined physical access points] to the facility where the system resides 24 hours per day, 7 days per week.	Functional	Intersects With	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	5		Not Selected
PE-03(04)	Physical Access Control | Lockable Casings	Use lockable physical casings to protect [Assignment: organization-defined system components] from unauthorized physical access.	Functional	Equal	Lockable Physical Casings	PES-03.2	Physical access control mechanisms exist to protect system components from unauthorized physical access (e.g., lockable physical casings).	10		Not Selected
PE-03(05)	Physical Access Control | Logical Tampering Protection	Employ [Assignment: organization-defined anti-tamper technologies] to [Selection (one or more): detect; prevent] physical tampering or alteration of [Assignment: organization-defined hardware components] within the system.	Functional	Equal	Mobile Device Tampering	MDM-04	Mechanisms exist to protect mobile devices from tampering through inspecting devices returning from locations that the organization deems to be of significant risk, prior to the device being connected to the organization's network.	10		Not Selected
PE-03(06)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
PE-03(07)	Physical Access Control | Physical Barriers	Limit access using physical barriers.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
PE-03(08)	Physical Access Control | Access Control Vestibules	Employ access control vestibules at [Assignment: organization-defined locations within the facility].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
PE-04	Access Control for Transmission	Control physical access to [Assignment: organization-defined system distribution and transmission lines] within organizational facilities using [Assignment: organization-defined security controls].	Functional	Equal	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or	10		Moderate
PE-05	Access Control for Output Devices	Control physical access to output from [Assignment: organization-defined output devices] to prevent unauthorized individuals from obtaining the output.	Functional	Equal	Access Control for Output Devices	PES-12.2	Physical security mechanisms exist to restrict access to printers and other system output devices to prevent unauthorized individuals from obtaining the output.	10		Moderate
PE-05(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
PE-05(02)	Access Control for Output Devices | Link to Individual Identity	Link individual identity to receipt of output from output devices.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
PE-05(03)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
PE-06	Monitoring Physical Access	a. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents;b. Review physical access logs [Assignment: organization-defined frequency] and upon occurrence of [Assignment: organization-defined events or potential indications of events]; andc. Coordinate results of reviews and investigations with the organizational incident response capability.	Functional	Equal	Monitoring Physical Access	PES-05	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.	10		Low
PE-06(01)	Monitoring Physical Access | Intrusion Alarms and Surveillance Equipment	Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment.	Functional	Equal	Intrusion Alarms / Surveillance Equipment	PES-05.1	Physical access control mechanisms exist to monitor physical intrusion alarms and surveillance equipment.	10		Moderate
PE-06(02)	Monitoring Physical Access | Automated Intrusion Recognition and Responses	Recognize [Assignment: organization-defined classes or types of intrusions] and initiate [Assignment: organization-defined response actions] using [Assignment: organization-defined automated mechanisms].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
PE-06(03)	Monitoring Physical Access | Video Surveillance	a. Employ video surveillance of [Assignment: organization-defined operational areas];b. Review video recordings [Assignment: organization-defined frequency]; andc. Retain video recordings for [Assignment: organization-defined time period].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
PE-06(04)	Monitoring Physical Access | Monitoring Physical Access to Systems	Monitor physical access to the system in addition to the physical access monitoring of the facility at [Assignment: organization-defined physical spaces containing one or more components of the system].	Functional	Equal	Monitoring Physical Access To Critical Systems	PES-05.2	Facility security mechanisms exist to monitor physical access to critical systems or sensitive/regulated data, in addition to the physical access monitoring of the facility.	10		High
PE-07		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
PE-08	Visitor Access Records	a. Maintain visitor access records to the facility where the system resides for [Assignment: organization-defined time period];b. Review visitor access records [Assignment: organization-defined frequency]; andc. Report anomalies in visitor access records to [Assignment: organization-defined personnel].	Functional	Equal	Physical Access Logs	PES-03.3	Physical access control mechanisms generate a log entry for each access attempt through controlled ingress and egress points.	10		Low
PE-08(01)	Visitor Access Records | Automated Records Maintenance and Review	Maintain and review visitor access records using [Assignment: organization-defined automated mechanisms].	Functional	Equal	Automated Records Management & Review	PES-06.4	Automated mechanisms exist to facilitate the maintenance and review of visitor access records.	10		High
PE-08(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
PE-08(03)	Visitor Access Records | Limit Personally Identifiable Information	Limit personally identifiable information contained in visitor access records to the following elements identified in the privacy risk assessment: [Assignment: organization-defined elements].	Functional	Equal	Minimize Visitor Personal Data (PD)	PES-06.5	Mechanisms exist to minimize the collection of Personal Data (PD) contained in visitor access records.	10		Not Selected

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-53B Baseline
PE-09	Power Equipment and Cabling	Protect power equipment and power cabling for the system from damage and destruction.	Functional	Equal	Supporting Utilities	PES-07	Facility security mechanisms exist to protect power equipment and power cabling for the system from damage and destruction.	10		Moderate
PE-09(01)	Power Equipment and Cabling | Redundant Cabling	Employ redundant power cabling paths that are physically separated by [Assignment: organization-defined distance].	Functional	Equal	Redundant Cabling	PES-07.7	Mechanisms exist to employ redundant power cabling paths that are physically separated to ensure that power continues to flow in the event one of the cables is cut or otherwise	10		Not Selected
PE-09(02)	Power Equipment and Cabling | Automatic Voltage Controls	Employ automatic voltage controls for [Assignment: organization-defined critical system components].	Functional	Equal	Automatic Voltage Controls	PES-07.1	Facility security mechanisms exist to utilize automatic voltage controls for critical system components.	10		Not Selected
PE-10	Emergency Shutoff	a. Provide the capability of shutting off power to [Assignment: organization-defined system or individual system components] in emergency situations;b. Place emergency shutoff switches or devices in [Assignment: organization-defined location by system or system component] to facilitate access for authorized personnel; andc. Protect emergency power shutoff capability from unauthorized activation.	Functional	Equal	Emergency Shutoff	PES-07.2	Facility security mechanisms exist to shut off power in emergency situations by: (1) Placing emergency shutoff switches or devices in close proximity to systems or system components to facilitate safe and easy access for personnel; and (2) Protecting emergency power shutoff capability from unauthorized activation.	10		Moderate
PE-10(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
PE-11	Emergency Power	Provide an uninterruptible power supply to facilitate [Selection (one or more): an orderly shutdown of the system; transition of the system to long-term alternate power] in the event of a primary power source loss.	Functional	Intersects With	Emergency Power	PES-07.3	Facility security mechanisms exist to supply alternate power, capable of maintaining minimally-required operational capability, in the event of an extended loss of the primary power source.	5		Moderate
PE-11(01)	Emergency Power | Alternate Power Supply — Minimal Operational Capability	Provide an alternate power supply for the system that is activated [Selection (one): manually; automatically] and that can maintain minimally required operational capability in the event of an extended loss of the primary power source.	Functional	Intersects With	Emergency Power	PES-07.3	Facility security mechanisms exist to supply alternate power, capable of maintaining minimally-required operational capability, in the event of an extended loss of the primary power source.	5		High
PE-11(02)	Emergency Power | Alternate Power Supply — Self-contained	Provide an alternate power supply for the system that is activated [Selection (one): manually; automatically] and that is:a. Self-contained;b. Not reliant on external power generation; andc. Capable of maintaining [Selection (one): minimally required operational capability; full operational capability] in the event of an extended loss of the primary power source.	Functional	Intersects With	Emergency Power	PES-07.3	Facility security mechanisms exist to supply alternate power, capable of maintaining minimally-required operational capability, in the event of an extended loss of the primary power source.	5		Not Selected
PE-12	Emergency Lighting	Employ and maintain automatic emergency lighting for the system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.	Functional	Equal	Emergency Lighting	PES-07.4	Facility security mechanisms exist to utilize and maintain automatic emergency lighting that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.	10		Low
PE-12(01)	Emergency Lighting | Essential Mission and Business Functions	Provide emergency lighting for all areas within the facility supporting essential mission and business functions.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
PE-13	Fire Protection	Employ and maintain fire detection and suppression systems that are supported by an independent energy source.	Functional	Equal	Fire Protection	PES-08	Facility security mechanisms exist to utilize and maintain fire suppression and detection devices/systems for the system that are supported by an independent energy source.	10		Low
PE-13(01)	Fire Protection | Detection Systems — Automatic Activation and Notification	Employ fire detection systems that activate automatically and notify [Assignment: organization-defined personnel or roles] and [Assignment: organization-defined emergency responders] in the event of a fire.	Functional	Equal	Fire Detection Devices	PES-08.1	Facility security mechanisms exist to utilize and maintain fire detection devices/systems that activate automatically and notify organizational personnel and emergency responders in the event of a fire.	10		Moderate
PE-13(02)	Fire Protection | Suppression Systems — Automatic Activation and Notification	a. Employ fire suppression systems that activate automatically and notify [Assignment: organization-defined personnel or roles] and [Assignment: organization-defined emergency responders]; andb. Employ an automatic fire suppression capability when the facility is not staffed on a continuous basis.	Functional	Intersects With	Automatic Fire Suppression	PES-08.3	Facility security mechanisms exist to employ an automatic fire suppression capability for critical systems when the facility is not staffed on a continuous basis.	5		High
PE-13(02)	Fire Protection | Suppression Systems — Automatic Activation and Notification	a. Employ fire suppression systems that activate automatically and notify [Assignment: organization-defined personnel or roles] and [Assignment: organization-defined emergency responders]; andb. Employ an automatic fire suppression capability when the facility is not staffed on a continuous basis.	Functional	Intersects With	Fire Suppression Devices	PES-08.2	Facility security mechanisms exist to utilize fire suppression devices/systems that provide automatic notification of any activation to organizational personnel and emergency responders.	5		High
PE-13(03)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
PE-13(04)	Fire Protection | Inspections	Ensure that the facility undergoes [Assignment: organization-defined frequency] fire protection inspections by authorized and qualified inspectors and identified deficiencies are resolved within [Assignment: organization-defined time period].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
PE-14	Environmental Controls	a. Maintain [Selection (one or more): temperature; humidity; pressure; radiation; [Assignment: organization-defined environmental control]] levels within the facility where the system resides at [Assignment: organization-defined acceptable levels]; andb. Monitor environmental control levels [Assignment: organization-defined frequency].	Functional	Equal	Temperature & Humidity Controls	PES-09	Facility security mechanisms exist to maintain and monitor temperature and humidity levels within the facility.	10		Low
PE-14(01)	Environmental Controls | Automatic Controls	Employ the following automatic environmental controls in the facility to prevent fluctuations potentially harmful to the system: [Assignment: organization-defined automatic environmental controls].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
PE-14(02)	Environmental Controls | Monitoring with Alarms and Notifications	Employ environmental control monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment to [Assignment: organization-defined personnel or roles].	Functional	Equal	Monitoring with Alarms / Notifications	PES-09.1	Facility security mechanisms exist to trigger an alarm or notification of temperature and humidity changes that be potentially harmful to personnel or equipment.	10		Not Selected
PE-15	Water Damage Protection	Protect the system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.	Functional	Equal	Water Damage Protection	PES-07.5	Facility security mechanisms exist to protect systems from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly and known to key personnel.	10		Low
PE-15(01)	Water Damage Protection | Automation Support	Detect the presence of water near the system and alert [Assignment: organization-defined personnel or roles] using [Assignment: organization-defined automated mechanisms].	Functional	Equal	Automation Support for Water Damage Protection	PES-07.6	Facility security mechanisms exist to detect the presence of water in the vicinity of critical systems and alert facility maintenance and IT personnel	10		High
PE-16	Delivery and Removal	a. Authorize and control [Assignment: organization-defined types of system components] entering and exiting the facility; andb. Maintain records of the system components.	Functional	Equal	Delivery & Removal	PES-10	Physical security mechanisms exist to isolate information processing facilities from points such as delivery and loading areas and other points to avoid unauthorized access.	10		Low
PE-17	Alternate Work Site	a. Determine and document the [Assignment: organization-defined alternate work sites] allowed for use by employees;b. Employ the following controls at alternate work sites: [Assignment: organization-defined controls];c. Assess the effectiveness of controls at alternate work sites; andd. Provide a means for employees to communicate with information security and privacy personnel in case of incidents.	Functional	Equal	Alternate Work Site	PES-11	Physical security mechanisms exist to utilize appropriate management, operational and technical controls at alternate work sites.	10		Moderate
PE-18	Location of System Components	Position 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.	Functional	Intersects With	Equipment Siting & Protection	PES-12	Physical security mechanisms exist to locate system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.	5		High
PE-18(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-53B Baseline
PE-19	Information Leakage	Protect the system from information leakage due to electromagnetic signals emanations.	Functional	Equal	Information Leakage Due To Electromagnetic Signals Emanations	PES-13	Facility security mechanisms exist to protect the system from information leakage due to electromagnetic signals emanations.	10		Not Selected
PE-19(01)	Information Leakage | National Emissions Policies and Procedures	Protect system components, associated data communications, and networks in accordance with national Emissions Security policies and procedures based on the security category or classification of the information.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
PE-20	Asset Monitoring and Tracking	Employ [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].	Functional	Equal	Asset Monitoring and Tracking	PES-14	Physical security mechanisms exist to employ asset location technologies that track and monitor the location and movement of organization-defined assets within organization-defined controlled areas.	10		Not Selected
PE-21	Electromagnetic Pulse Protection	Employ [Assignment: organization-defined protective measures] against electromagnetic pulse damage for [Assignment: organization-defined systems and system components].	Functional	Equal	Electromagnetic Pulse (EMP) Protection	PES-15	Physical security mechanisms exist to employ safeguards against Electromagnetic Pulse (EMP) damage for systems and system components.	10		Not Selected
PE-22	Component Marking	Mark [Assignment: organization-defined system hardware components] indicating the impact level or classification level of the information permitted to be processed, stored, or transmitted by the hardware component.	Functional	Intersects With	Asset Scope Classification	AST-04.1	Mechanisms exist to determine security, compliance and resilience control applicability by identifying, assigning and documenting the appropriate asset scope categorization for all Technology Assets, Applications and/or Services (TAAS) and personnel (internal and third-party).	5		Not Selected
PE-22	Component Marking	Mark [Assignment: organization-defined system hardware components] indicating the impact level or classification level of the information permitted to be processed, stored, or transmitted by the hardware component.	Functional	Intersects With	Component Marking	PES-16	Physical security mechanisms exist to mark system hardware components indicating the impact or classification level of the information permitted to be processed, stored or transmitted by the hardware component.	5		Not Selected
PE-23	Facility Location	a. Plan the location or site of the facility where the system resides considering physical and environmental hazards; andb. For existing facilities, consider the physical and environmental hazards in the organizational risk management strategy.	Functional	Intersects With	Third-Party Processing, Storage and Service Locations	TPM-04.4	Mechanisms exist to restrict the location of information processing/storage based on business requirements.	5		Not Selected
PE-23	Facility Location	a. Plan the location or site of the facility where the system resides considering physical and environmental hazards; andb. For existing facilities, consider the physical and environmental hazards in the organizational risk management strategy.	Functional	Intersects With	Alternate Processing Site	BCD-09	Mechanisms exist to establish an alternate processing site that provides security measures equivalent to that of the primary site.	5		Not Selected
PE-23	Facility Location	a. Plan the location or site of the facility where the system resides considering physical and environmental hazards; andb. For existing facilities, consider the physical and environmental hazards in the organizational risk management strategy.	Functional	Intersects With	Alternate Storage Site	BCD-08	Mechanisms exist to establish an alternate storage site that includes both the assets and necessary agreements to permit the storage and recovery of system backup information.	5		Not Selected
PE-23	Facility Location	a. Plan the location or site of the facility where the system resides considering physical and environmental hazards; andb. For existing facilities, consider the physical and environmental hazards in the organizational risk management strategy.	Functional	Intersects With	Distributed Processing & Storage	SEA-15	Mechanisms exist to distribute processing and storage across multiple physical locations.	5		Not Selected
PE-23	Facility Location	a. Plan the location or site of the facility where the system resides considering physical and environmental hazards; andb. For existing facilities, consider the physical and environmental hazards in the organizational risk management strategy.	Functional	Intersects With	Equipment Siting & Protection	PES-12	Physical security mechanisms exist to locate system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.	5		Not Selected
PE-23	Facility Location	a. Plan the location or site of the facility where the system resides considering physical and environmental hazards; andb. For existing facilities, consider the physical and environmental hazards in the organizational risk management strategy.	Functional	Intersects With	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	5		Not Selected
PL-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] planning policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the planning policy and the associated planning controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the planning policy and procedures; andc. Review and update the current planning:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Subset Of	Security, Compliance & Resilience Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance and resilience objectives.	10		Low
PL-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] planning policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the planning policy and the associated planning controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the planning policy and procedures; andc. Review and update the current planning:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10		Low
PL-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] planning policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the planning policy and the associated planning controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the planning policy and procedures; andc. Review and update the current planning:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Subset Of	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	10		Low

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-53B Baseline
PL-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] planning policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the planning policy and the associated planning controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the planning policy and procedures; andc. Review and update the current planning:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events];d. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] planning policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the planning policy and the associated planning controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the planning policy and procedures; andc. Review and update the current planning:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events];	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5		Low
PL-01	Policy and Procedures		Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5		Low
PL-02	System Security and Privacy Plans	enterprise architecture;2. Explicitly define the constituent system components;3. Describe the operational context of the system in terms of mission and business processes;4. Identify the individuals that fulfill system roles and responsibilities;5. Identify the information types processed, stored, and transmitted by the system;6. Provide the security categorization of the system, including supporting rationale;7. Describe any specific threats to the system that are of concern to the organization;8. Provide the results of a privacy risk assessment for systems processing personally identifiable information;9. Describe the operational environment for the system and any dependencies on or connections to other systems or system components;10. Provide an overview of the security and privacy requirements for the system;11. Identify any relevant control baselines or overlays, if applicable;12. Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions;13. Include risk determinations for security and privacy architecture and design decisions;14. Include security- and privacy-related activities affecting the system that require planning and coordination with [Assignment: organization-defined individuals or groups]; and15. Are reviewed and approved by the authorizing official or designated representative prior to plan implementation.b. Distribute copies of the plans and communicate subsequent changes to the plans to [Assignment: organization-defined personnel or roles];c. Review the plans [Assignment: organization-defined frequency];d. Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments;	Functional	Intersects With	Plan / Coordinate with Other Organizational Entities	IAO-03.1	Mechanisms exist to plan and coordinate Information Assurance Program (IAP) activities with affected stakeholders before conducting such activities in order to reduce the potential impact on operations.	5		Low
PL-02	System Security and Privacy Plans	enterprise architecture;2. Explicitly define the constituent system components;3. Describe the operational context of the system in terms of mission and business processes;4. Identify the individuals that fulfill system roles and responsibilities;5. Identify the information types processed, stored, and transmitted by the system;6. Provide the security categorization of the system, including supporting rationale;7. Describe any specific threats to the system that are of concern to the organization;8. Provide the results of a privacy risk assessment for systems processing personally identifiable information;9. Describe the operational environment for the system and any dependencies on or connections to other systems or system components;10. Provide an overview of the security and privacy requirements for the system;11. Identify any relevant control baselines or overlays, if applicable;12. Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions;13. Include risk determinations for security and privacy architecture and design decisions;14. Include security- and privacy-related activities affecting the system that require planning and coordination with [Assignment: organization-defined individuals or groups]; and15. Are reviewed and approved by the authorizing official or designated representative prior to plan implementation.b. Distribute copies of the plans and communicate subsequent changes to the plans to [Assignment: organization-defined personnel or roles];c. Review the plans [Assignment: organization-defined frequency];d. Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments;	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and (3) Provides a historical record of applied security controls, including changes.	5		Low
PL-02	System Security and Privacy Plans	enterprise architecture;2. Explicitly define the constituent system components;3. Describe the operational context of the system in terms of mission and business processes;4. Identify the individuals that fulfill system roles and responsibilities;5. Identify the information types processed, stored, and transmitted by the system;6. Provide the security categorization of the system, including supporting rationale;7. Describe any specific threats to the system that are of concern to the organization;8. Provide the results of a privacy risk assessment for systems processing personally identifiable information;9. Describe the operational environment for the system and any dependencies on or connections to other systems or system components;10. Provide an overview of the security and privacy requirements for the system;11. Identify any relevant control baselines or overlays, if applicable;12. Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions;13. Include risk determinations for security and privacy architecture and design decisions;14. Include security- and privacy-related activities affecting the system that require planning and coordination with [Assignment: organization-defined individuals or groups]; and15. Are reviewed and approved by the authorizing official or designated representative prior to plan implementation.b. Distribute copies of the plans and communicate subsequent changes to the plans to [Assignment: organization-defined personnel or roles];c. Review the plans [Assignment: organization-defined frequency];d. Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments;	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive/regulated data flows.	5		Low
PL-02(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-53B Baseline
PL-02(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
PL-02(03)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
PL-03		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
PL-04	Rules of Behavior	a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy;b. Receive a documented acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system;c. Review and update the rules of behavior [Assignment: organization-defined frequency]; andd. Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge [Selection (one or more): [Assignment: organization-defined frequency]; when the rules are revised or updated].	Functional	Intersects With	Terms of Employment	HRS-05	Mechanisms exist to require all employees and contractors to apply cybersecurity and data protection principles in their daily work to enable secure, compliant and resilient capabilities.	5		Low
PL-04	Rules of Behavior	a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy;b. Receive a documented acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system;c. Review and update the rules of behavior [Assignment: organization-defined frequency]; andd. Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge [Selection (one or more): [Assignment: organization-defined frequency]; when the rules are revised or updated].	Functional	Intersects With	Rules of Behavior	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	5		Low
PL-04	Rules of Behavior	a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy;b. Receive a documented acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system;c. Review and update the rules of behavior [Assignment: organization-defined frequency]; andd. Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge [Selection (one or more): [Assignment: organization-defined frequency]; when the rules are revised or updated].	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.	5		Low
PL-04(01)	Rules of Behavior | Social Media and External Site/application Usage Restrictions	Include in the rules of behavior, restrictions on:a. Use of social media, social networking sites, and external sites/applications;b. Posting organizational information on public websites; andc. Use of organization-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications.	Functional	Equal	Social Media & Social Networking Restrictions	HRS-05.2	Mechanisms exist to define rules of behavior that contain explicit restrictions on the use of social media and networking sites, posting information on commercial websites and sharing account information.	10		Low
PL-05		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
PL-06		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
PL-07	Concept of Operations	a. Develop a Concept of Operations (CONOPS) for the system describing how the organization intends to operate the system from the perspective of information security and privacy; andb. Review and update the CONOPS [Assignment: organization-defined frequency].	Functional	Equal	Security Concept Of Operations (CONOPS)	OPS-02	Mechanisms exist to develop a security Concept of Operations (CONOPS), or a similarly-defined plan for achieving cybersecurity objectives, that documents management, operational and technical measures implemented to apply defense-in-depth techniques that is communicated to all appropriate stakeholders.	10		Not Selected
PL-08	Security and Privacy Architectures	system that:1. Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information;2. Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals;3. Describe how the architectures are integrated into and support the enterprise architecture; and4. Describe any assumptions about, and dependencies on, external systems and services;b. Review and update the architectures [Assignment: organization-defined frequency] to reflect changes in the enterprise architecture; andc. Reflect planned architecture changes in security and privacy plans, Concept of Operations (CONOPS), criticality analysis, organizational procedures, and procurements and	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations.	5		Moderate
PL-08(01)	Security and Privacy Architectures | Defense in Depth	Design the security and privacy architectures for the system using a defense-in-depth approach that:a. Allocates [Assignment: organization-defined controls] to [Assignment: organization-defined locations and architectural layers]; andb. Ensures that the allocated controls operate in a coordinated and mutually reinforcing manner.	Functional	Intersects With	Defense-In-Depth (DiD) Architecture	SEA-03	Mechanisms exist to implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.	5		Not Selected
PL-08(02)	Security and Privacy Architectures | Supplier Diversity	Require that [Assignment: organization-defined controls] allocated to [Assignment: organization-defined locations and architectural layers] are obtained from different suppliers.	Functional	Intersects With	Supplier Diversity	TDA-03.1	Mechanisms exist to obtain security, compliance and resilience technologies from different suppliers to minimize supply chain risk.	5		Not Selected
PL-09	Central Management	Centrally manage [Assignment: organization-defined controls and related processes].	Functional	Intersects With	Centralized Management of Security, Compliance & Resilience Controls	SEA-01.1	Mechanisms exist to centrally-manage the organization-wide management and implementation of security, compliance and resilience controls and related processes.	5		Not Selected
PL-09	Central Management	Centrally manage [Assignment: organization-defined controls and related processes].	Functional	Intersects With	Centralized Management of Flaw Remediation Processes	VPM-05.1	Mechanisms exist to centrally-manage the flaw remediation process.	5		Not Selected
PL-09	Central Management	Centrally manage [Assignment: organization-defined controls and related processes].	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5		Not Selected
PL-09	Central Management	Centrally manage [Assignment: organization-defined controls and related processes].	Functional	Intersects With	Centralized Management of Antimalware Technologies	END-04.3	Mechanisms exist to centrally-manage antimalware technologies.	5		Not Selected
PL-09	Central Management	Centrally manage [Assignment: organization-defined controls and related processes].	Functional	Intersects With	Central Management	END-08.1	Mechanisms exist to centrally-manage anti-phishing and spam protection technologies.	5		Not Selected
PL-09	Central Management	Centrally manage [Assignment: organization-defined controls and related processes].	Functional	Intersects With	Centralized Management of Event Log Content	MON-03.6	Mechanisms exist to centrally manage and update the criteria to be captured in event logs generated by organization-defined system components.	5		Not Selected
PL-10	Baseline Selection	Select a control baseline for the system.	Functional	Equal	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening	10		Low

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh	Notes	NIST SP 800-53B Baseline
PL-11	Baseline Tailoring	Tailor the selected control baseline by applying specified tailoring actions.	Functional	Equal	Baseline Tailoring	CFG-02.9	Mechanisms exist to allow baseline controls to be specialized or customized by applying a defined set of tailoring actions that are specific to: (1) Mission / business functions; (2) Operational environment; (3) Specific threats or vulnerabilities; or (4) Other conditions or situations that could affect mission / business success.	10		Low
PM-01	Information Security Program Plan	a. Develop and disseminate an organization-wide information security program plan that:1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance;3. Reflects the coordination among organizational entities responsible for information security; and4. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation;b. Review and update the organization-wide information security program plan [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; andc. Protect the information security program plan from unauthorized disclosure and modification.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10		Not Associated
PM-01	Information Security Program Plan	a. Develop and disseminate an organization-wide information security program plan that:1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance;3. Reflects the coordination among organizational entities responsible for information security; and4. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation;b. Review and update the organization-wide information security program plan [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; andc. Protect the information security program plan from unauthorized disclosure and modification.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5		Not Associated
PM-01	Information Security Program Plan	a. Develop and disseminate an organization-wide information security program plan that:1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance;3. Reflects the coordination among organizational entities responsible for information security; and4. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation;b. Review and update the organization-wide information security program plan [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; andc. Protect the information security program plan from unauthorized disclosure and modification.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5		Not Associated
PM-02	Information Security Program Leadership Role	Appoint a senior agency information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5		Not Associated
PM-03	Information Security and Privacy Resources	a. Include the resources needed to implement the information security and privacy programs in capital planning and investment requests and document all exceptions to this requirement;b. Prepare documentation required for addressing information security and privacy programs in capital planning and investment requests in accordance with applicable laws, executive orders, directives, policies, regulations, standards; andc. Make available for expenditure, the planned information security and privacy resources.	Functional	Equal	Security, Compliance & Resilience Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the Security, Compliance & Resilience Program (SCRP) and document all exceptions to this requirement.	10		Not Associated
PM-04	Plan of Action and Milestones Process	a. Implement a process to ensure that plans of action and milestones for the information security, privacy, and supply chain risk management programs and associated organizational systems:1. Are developed and maintained;2. Document the remedial information security, privacy, and supply chain risk management actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and3. Are reported in accordance with established reporting requirements.b. Review plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5		Not Associated
PM-04	Plan of Action and Milestones Process	a. Implement a process to ensure that plans of action and milestones for the information security, privacy, and supply chain risk management programs and associated organizational systems:1. Are developed and maintained;2. Document the remedial information security, privacy, and supply chain risk management actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and3. Are reported in accordance with established reporting requirements.b. Review plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.	Functional	Intersects With	Capabilities Deficiency Tracking	IAO-05	(2) Applicable security, compliance and/or resilience control; (3) Description of the deficiency(ies); (4) Risk associated with the deficiency(ies); (5) Source deficiency identification/detection; (6) Temporary compensating controls, if applicable; (7) Point of Contact (POC) (e.g., asset/process owner); (8) Resources required to	5		Not Associated
PM-05	System Inventory	Develop and update [Assignment: organization-defined frequency] an inventory of organizational systems.	Functional	Intersects With	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	5		Not Associated
PM-05	System Inventory	Develop and update [Assignment: organization-defined frequency] an inventory of organizational systems.	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	5		Not Associated

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh	Notes	NIST SP 800-53B Baseline
PM-05(01)	System Inventory | Inventory of Personally Identifiable Information	Establish, maintain, and update [Assignment: organization-defined frequency] an inventory of all systems, applications, and projects that process personally identifiable information.	Functional	Intersects With	Inventory of Personal Data (PD)	PRI-05.5	Mechanisms exist to establish and maintain a current inventory of all Technology Assets, Applications and/or Services (TAAS) that collect, receive, process, store, transmit, share, update and/or dispose Personal	5		Not Associated
PM-05(01)	Inventory of Personally Identifiable	Establish, maintain, and update [Assignment: organization-defined frequency] an inventory of all systems, applications, and projects that process personally identifiable information.	Functional	Intersects With	Personal Data (PD) Inventory Automation Support	PRI-05.6	Automated mechanisms exist to determine if Personal Data (PD) is maintained in electronic form.	5		Not Associated
PM-06	Measures of Performance	Develop, monitor, and report on the results of information security and privacy measures of performance.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5		Not Associated
PM-06	Measures of Performance	Develop, monitor, and report on the results of information security and privacy measures of performance.	Functional	Intersects With	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	5		Not Associated
PM-07	Enterprise Architecture	Develop and maintain an enterprise architecture with consideration for information security, privacy, and the resulting risk to organizational operations and assets, individuals, other organizations, and the Nation.	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations.	5		Not Associated
PM-07(01)	Enterprise Architecture | Offloading	Offload [Assignment: organization-defined non-essential functions or services] to other systems, system components, or an external provider.	Functional	Equal	Outsourcing Non-Essential Functions or Services	SEA-02.2	Mechanisms exist to identify non-essential functions or services that are capable of being outsourced to external service providers and align with the organization's enterprise architecture and security standards.	10		Not Associated
PM-08	Critical Infrastructure Plan	Address information security and privacy issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	5		Not Associated
PM-08	Critical Infrastructure Plan	Address information security and privacy issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5		Not Associated
PM-09	Risk Management Strategy	Security risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of organizational systems; and2. Privacy risk to individuals resulting from the authorized processing of personally identifiable information;b. Implement the risk management strategy consistently across the organization; andc. Review and update the risk management strategy [Assignment: organization-defined frequency] or as required, to address	Functional	Equal	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10		Not Associated
PM-10	Authorization Process	a. Manage the security and privacy state of organizational systems and the environments in which those systems operate through authorization processes;b. Designate individuals to fulfill specific roles and responsibilities within the organizational risk management process; andc. Integrate the authorization processes into an organization-wide risk management program.	Functional	Equal	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10		Not Associated
PM-11	Mission and Business Process Definition	a. Define organizational mission and business processes with consideration for information security and privacy and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; andb. Determine information protection and personally identifiable information processing needs arising from the defined mission and business processes; andc. Review and revise the mission and business processes [Assignment: organization-defined frequency].	Functional	Equal	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and (2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	10		Not Associated
PM-12	Insider Threat Program	Implement an insider threat program that includes a cross-discipline insider threat incident handling team.	Functional	Equal	Insider Threat Program	THR-04	Mechanisms exist to implement an insider threat program that includes a cross-discipline insider threat incident handling team.	10		Not Associated
PM-13	Security and Privacy Workforce	Establish a security and privacy workforce development and improvement program.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5		Not Associated
PM-13	Security and Privacy Workforce	Establish a security and privacy workforce development and improvement program.	Functional	Intersects With	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	5		Not Associated
PM-14	Testing, Training, and Monitoring	a. Implement a process for ensuring that organizational plans for conducting security and privacy testing, training, and monitoring activities associated with organizational systems:1. Are developed and maintained; and2. Continue to be executed; andb. Review testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.	Functional	Intersects With	Personal Data (PD) Control Testing, Training & Monitoring	PRI-08	Mechanisms exist to conduct testing, training and monitoring activities for Personal Data (PD) controls.	5		Not Associated
PM-14	Testing, Training, and Monitoring	a. Implement a process for ensuring that organizational plans for conducting security and privacy testing, training, and monitoring activities associated with organizational systems:1. Are developed and maintained; and2. Continue to be executed; andb. Review testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5		Not Associated
PM-15	Security and Privacy Groups and Associations	Establish and institutionalize contact with selected groups and associations within the security and privacy communities:a. To facilitate ongoing security and privacy education and training for organizational personnel;b. To maintain currency with recommended security and privacy practices, techniques, and technologies; andc. To share current security and privacy information, including threats, vulnerabilities, and incidents.	Functional	Intersects With	Threat Intelligence Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	5		Not Associated
PM-15	Security and Privacy Groups and Associations	Establish and institutionalize contact with selected groups and associations within the security and privacy communities:a. To facilitate ongoing security and privacy education and training for organizational personnel;b. To maintain currency with recommended security and privacy practices, techniques, and technologies; andc. To share current security and privacy information, including threats, vulnerabilities, and incidents.	Functional	Intersects With	Contacts With Groups & Associations	GOV-07	Mechanisms exist to establish contact with selected groups and associations within the security, compliance and resilience communities to: (1) Facilitate ongoing cybersecurity and data protection education and training for organizational personnel; (2) Maintain currency with recommended cybersecurity and data protection practices, techniques and technologies; and (3) Share current cybersecurity and/or data protection-related information including threats, vulnerabilities and incidents.	5		Not Associated

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh	Notes	NIST SP 800-53B Baseline
PM-16	Threat Awareness Program	Implement a threat awareness program that includes a cross-organization information-sharing capability for threat intelligence.	Functional	Intersects With	Threat Intelligence Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	5		Not Associated
PM-16(01)	Threat Awareness Program | Automated Means for Sharing Threat Intelligence Feeds	Employ automated mechanisms to maximize the effectiveness of sharing threat intelligence information.	Functional	Intersects With	Threat Intelligence Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5		Not Associated
PM-17	Protecting Controlled Unclassified Information on External Systems	a. Establish policy and procedures to ensure that requirements for the protection of controlled unclassified information that is processed, stored or transmitted on external systems, are implemented in accordance with applicable laws, executive orders, directives, policies, regulations, and standards; andb. Review and update the policy and procedures [Assignment: organization-defined frequency].	Functional	Equal	Protecting Sensitive / Regulated Data on External Technology Assets, Applications and/or Services (TAAS)	DCH-13.3	Mechanisms exist to ensure that the requirements for the protection of sensitive/regulated data processed, stored or transmitted on external Technology Assets, Applications and/or Services (TAAS), are implemented in accordance with applicable statutory, regulatory	10		Not Associated
PM-18	Privacy Program Plan	a. Develop and disseminate an organization-wide privacy program plan that provides an overview of the agency's privacy program, and:1. Includes a description of the structure of the privacy program and the resources dedicated to the privacy program;2. Provides an overview of the requirements for the privacy program and a description of the privacy program management controls and common controls in place or planned for meeting those requirements;3. Includes the role of the senior agency official for privacy and the identification and assignment of roles of other privacy officials and staff and their responsibilities;4. Describes management commitment, compliance, and the strategic goals and objectives of the privacy program;5. Reflects coordination among organizational entities responsible for the different aspects of privacy; and6. Is approved by a senior official with responsibility and accountability for the privacy risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; andb. Update the plan [Assignment: organization-defined frequency] and to address changes in federal privacy laws and policy and organizational changes and problems identified during plan implementation or privacy control assessments.	Functional	Equal	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	10		Not Associated
PM-19	Privacy Program Leadership Role	Appoint a senior agency official for privacy with the authority, mission, accountability, and resources to coordinate, develop, and implement, applicable privacy requirements and manage privacy risks through the organization-wide privacy program.	Functional	Equal	Chief Privacy Officer (CPO)	PRI-01.1	Mechanisms exist to appoints a Chief Privacy Officer (CPO) or similar role, with the authority, mission, accountability and resources to coordinate, develop and implement, applicable data privacy requirements and manage data privacy risks through the organization-wide data privacy program.	10		Not Associated
PM-20	Dissemination of Privacy Program Information	Maintain a central resource webpage on the organization's principal public website that serves as a central source of information about the organization's privacy program and that:a. Ensures that the public has access to information about organizational privacy activities and can communicate with its senior agency official for privacy;b. Ensures that organizational privacy practices and reports are publicly available; andc. Employs publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to privacy offices regarding privacy practices.	Functional	Equal	Dissemination of Data Privacy Program Information	PRI-01.3	Mechanisms exist to: (1) Ensure that the public has access to information about organizational data privacy activities and can communicate with its Chief Privacy Officer (CPO) or similar role; (2) Ensure that organizational data privacy practices are publicly available through organizational websites or document repositories; (3) Utilize publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to data privacy office(s) regarding data privacy practices; and (4) Inform data subjects when changes are made to the privacy notice and the nature of such changes.	10		Not Associated
PM-20(01)	Dissemination of Privacy Program Information | Privacy Policies on Websites, Applications, and Digital Services	Develop and post privacy policies on all external-facing websites, mobile applications, and other digital services, that:a. Are written in plain language and organized in a way that is easy to understand and navigate;b. Provide information needed by the public to make an informed decision about whether and how to interact with the organization; andc. Are updated whenever the organization makes a substantive change to the practices it describes and includes a time/date stamp to inform the public of the date of the most recent changes.	Functional	Equal	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations; (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and	10		Not Associated
PM-21	Accounting of Disclosures	a. Develop and maintain an accurate accounting of disclosures of personally identifiable information, including:1. Date, nature, and purpose of each disclosure; and2. Name and address, or other contact information of the individual or organization to which the disclosure was made;b. Retain the accounting of disclosures for the length of the time the personally identifiable information is maintained or five years after the disclosure is made, whichever is longer; andc. Make the accounting of disclosures available to the individual to whom the personally identifiable information relates upon request.	Functional	Equal	Accounting of Disclosures	PRI-14.1	Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by: (1) The organization; and/or (2) Relevant third-parties that their PD was shared with.	10		Not Associated
PM-22	Personally Identifiable Information Quality Management	Develop and document organization-wide policies and procedures for:a. Reviewing for the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle;b. Correcting or deleting inaccurate or outdated personally identifiable information;c. Disseminating notice of corrected or deleted personally identifiable information to individuals or other appropriate entities; andd. Appeals of adverse decisions on correction or deletion requests.	Functional	Intersects With	Data Quality Management	PRI-10	Mechanisms exist to manage the quality, utility, objectivity, integrity and impact determination and de-identification of sensitive/regulated data across the information lifecycle.	5		Not Associated
PM-22	Personally Identifiable Information Quality Management	Develop and document organization-wide policies and procedures for:a. Reviewing for the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle;b. Correcting or deleting inaccurate or outdated personally identifiable information;c. Disseminating notice of corrected or deleted personally identifiable information to individuals or other appropriate entities; andd. Appeals of adverse decisions on correction or deletion requests.	Functional	Intersects With	Data Quality Operations	DCH-22	Mechanisms exist to check for Redundant, Obsolete/Outdated, Toxic or Trivial (ROTT) data to ensure the accuracy, relevance, timeliness, impact, completeness and de-identification of information throughout the information lifecycle.	5		Not Associated

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh	Notes	NIST SP 800-53B Baseline
PM-23	Data Governance Body	Establish a Data Governance Body consisting of [Assignment: organization-defined roles] with [Assignment: organization-defined responsibilities].	Functional	Intersects With	Data Management Board	PRI-13	Mechanisms exist to establish a written charter for a Data Management Board (DMB) and assigned organization-defined roles to the DMB.	5		Not Associated
PM-23	Data Governance Body	Establish a Data Governance Body consisting of [Assignment: organization-defined roles] with [Assignment: organization-defined responsibilities].	Functional	Intersects With	Data Quality Management	PRI-10	Mechanisms exist to manage the quality, utility, objectivity, integrity and impact determination and de-identification of sensitive/regulated data across the information lifecycle.	5		Not Associated
PM-23	Data Governance Body	Establish a Data Governance Body consisting of [Assignment: organization-defined roles] with [Assignment: organization-defined responsibilities].	Functional	Intersects With	Data Governance	GOV-10	Mechanisms exist to facilitate data governance to oversee the organization's policies, standards and procedures so that sensitive/regulated data is effectively managed and maintained in accordance with applicable statutory, regulatory and contractual obligations.	5		Not Associated
PM-24	Data Integrity Board	Establish a Data Integrity Board to:a. Review proposals to conduct or participate in a matching program; andb. Conduct an annual review of all matching programs in which the agency has participated.	Functional	Intersects With	Data Governance	GOV-10	Mechanisms exist to facilitate data governance to oversee the organization's policies, standards and procedures so that sensitive/regulated data is effectively managed and maintained in accordance with applicable statutory, regulatory and contractual obligations.	5		Not Associated
PM-24	Data Integrity Board	Establish a Data Integrity Board to:a. Review proposals to conduct or participate in a matching program; andb. Conduct an annual review of all matching programs in which the agency has participated.	Functional	Intersects With	Data Management Board	PRI-13	Mechanisms exist to establish a written charter for a Data Management Board (DMB) and assigned organization-defined roles to the DMB.	5		Not Associated
PM-24	Data Integrity Board	Establish a Data Integrity Board to:a. Review proposals to conduct or participate in a matching program; andb. Conduct an annual review of all matching programs in which the agency has participated.	Functional	Intersects With	Data Quality Management	PRI-10	Mechanisms exist to manage the quality, utility, objectivity, integrity and impact determination and de-identification of sensitive/regulated data across the information lifecycle.	5		Not Associated
PM-24	Data Integrity Board	Establish a Data Integrity Board to:a. Review proposals to conduct or participate in a matching program; andb. Conduct an annual review of all matching programs in which the agency has participated.	Functional	Intersects With	Personal Data (PD) Accuracy & Integrity	PRI-05.2	Mechanisms exist to ensure the accuracy and relevance of Personal Data (PD) throughout the information lifecycle by: (1) Keeping PD up-to-date; and	5		Not Associated
PM-24	Data Integrity Board	Establish a Data Integrity Board to:a. Review proposals to conduct or participate in a matching program; andb. Conduct an annual review of all matching programs in which the agency has participated.	Functional	Intersects With	Computer Matching Agreements (CMA)	PRI-02.3	Mechanisms exist to publish Computer Matching Agreements (CMA) on the organization's public website(s).	5		Not Associated
PM-24	Data Integrity Board	Establish a Data Integrity Board to:a. Review proposals to conduct or participate in a matching program; andb. Conduct an annual review of all matching programs in which the agency has participated.	Functional	Intersects With	Automated Data Management Processes	PRI-02.2	Automated mechanisms exist to adjust data that is able to be collected, received, processed, stored, transmitted, shared, updated and/or disposed, based on updated data subject authorization(s).	5		Not Associated
PM-25	Minimization of Personally Identifiable Information Used in Testing, Training, and Research	a. Develop, document, and implement policies and procedures that address the use of personally identifiable information for internal testing, training, and research;b. Limit or minimize the amount of personally identifiable information used for internal testing, training, and research purposes;c. Authorize the use of personally identifiable information when such information is required for internal testing, training, and research; andd. Review and update policies and procedures [Assignment: organization-defined frequency].	Functional	Intersects With	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to: (1) The purpose(s) originally collected, consistent with the data privacy notice(s); (2) What is authorized by the data subject, or authorized agent; and	5		Not Associated
PM-25	Minimization of Personally Identifiable Information Used in Testing, Training, and Research	a. Develop, document, and implement policies and procedures that address the use of personally identifiable information for internal testing, training, and research;b. Limit or minimize the amount of personally identifiable information used for internal testing, training, and research purposes;c. Authorize the use of personally identifiable information when such information is required for internal testing, training, and research; andd. Review and update policies and procedures [Assignment: organization-defined frequency].	Functional	Intersects With	Collection Minimization	END-13.3	Mechanisms exist to utilize sensors that are configured to minimize the collection of information about individuals.	5		Not Associated
PM-25	Minimization of Personally Identifiable Information Used in Testing, Training, and Research	a. Develop, document, and implement policies and procedures that address the use of personally identifiable information for internal testing, training, and research;b. Limit or minimize the amount of personally identifiable information used for internal testing, training, and research purposes;c. Authorize the use of personally identifiable information when such information is required for internal testing, training, and research; andd. Review and update policies and procedures [Assignment: organization-defined frequency].	Functional	Intersects With	Minimize Visitor Personal Data (PD)	PES-06.5	Mechanisms exist to minimize the collection of Personal Data (PD) contained in visitor access records.	5		Not Associated
PM-25	Minimization of Personally Identifiable Information Used in Testing, Training, and Research	a. Develop, document, and implement policies and procedures that address the use of personally identifiable information for internal testing, training, and research;b. Limit or minimize the amount of personally identifiable information used for internal testing, training, and research purposes;c. Authorize the use of personally identifiable information when such information is required for internal testing, training, and research; andd. Review and update policies and procedures [Assignment: organization-defined frequency].	Functional	Intersects With	Internal Use of Personal Data (PD) For Testing, Training and Research	PRI-05.1	Mechanisms exist to address the use of Personal Data (PD) for internal testing, training and research that: (1) Takes measures to limit or minimize the amount of PD used for internal testing, training and research purposes; and (2) Authorizes the use of PD when such information is required for internal testing, training and research.	5		Not Associated
PM-25	Minimization of Personally Identifiable Information Used in Testing, Training, and Research	a. Develop, document, and implement policies and procedures that address the use of personally identifiable information for internal testing, training, and research;b. Limit or minimize the amount of personally identifiable information used for internal testing, training, and research purposes;c. Authorize the use of personally identifiable information when such information is required for internal testing, training, and research; andd. Review and update policies and procedures [Assignment: organization-defined frequency].	Functional	Intersects With	Limit Sensitive / Regulated Data In Testing, Training & Research	DCH-18.2	Mechanisms exist to minimize the use of sensitive/regulated data for research, testing, or training, in accordance with authorized, legitimate business practices.	5		Not Associated
PM-26	Complaint Management	Implement a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational security and privacy practices that includes:a. Mechanisms that are easy to use and readily accessible by the public;b. All information necessary for successfully filing complaints;c. Tracking mechanisms to ensure all complaints received are reviewed and addressed within [Assignment: organization-defined time period];d. Acknowledgement of receipt of complaints, concerns, or questions from individuals within [Assignment: organization-defined time period]; ande. Response to complaints, concerns, or questions from individuals within [Assignment: organization-defined time period].	Functional	Intersects With	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	5		Not Associated
PM-26	Complaint Management	Implement a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational security and privacy practices that includes:a. Mechanisms that are easy to use and readily accessible by the public;b. All information necessary for successfully filing complaints;c. Tracking mechanisms to ensure all complaints received are reviewed and addressed within [Assignment: organization-defined time period];d. Acknowledgement of receipt of complaints, concerns, or questions from individuals within [Assignment: organization-defined time period]; ande. Response to complaints, concerns, or questions from individuals within [Assignment: organization-defined time period].	Functional	Intersects With	Appeal Adverse Decision	PRI-06.3	Mechanisms exist to maintain a process for data subjects to appeal an adverse decision.	5		Not Associated

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-53B Baseline
PM-27	Privacy Reporting	a. Develop [Assignment: organization-defined privacy reports] and disseminate to:1. [Assignment: organization-defined oversight bodies] to demonstrate accountability with statutory, regulatory, and policy privacy mandates; and2. [Assignment: organization-defined officials] and other personnel with responsibility for monitoring privacy program compliance; andb. Review and update privacy reports [Assignment: organization-defined frequency].	Functional	Equal	Documenting Data Processing Activities	PRI-14	Mechanisms exist to document Personal Data (PD) processing activities that covers collection, receiving, processing, storage, transmission, sharing, updating and/or disposal actions with sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual requirements.	10		Not Associated
PM-28	Risk Framing	a. Identify and document:1. Assumptions affecting risk assessments, risk responses, and risk monitoring;2. Constraints affecting risk assessments, risk responses, and risk monitoring;3. Priorities and trade-offs considered by the organization for managing risk; and4. Organizational risk tolerance;b. Distribute the results of risk framing activities to [Assignment: organization-defined personnel]; andc. Review and update risk framing considerations [Assignment: organization-defined frequency].	Functional	Equal	Risk Framing	RSK-01.1	Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Constraints affecting risk assessments, risk response and risk monitoring; (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing risk.	10		Not Associated
PM-29	Risk Management Program Leadership Roles	a. Appoint a Senior Accountable Official for Risk Management to align organizational information security and privacy management processes with strategic, operational, and budgetary planning processes; andb. Establish a Risk Executive (function) to view and analyze risk from an organization-wide perspective and ensure management of risk is consistent across the organization.	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against	5		Not Associated
PM-29	Risk Management Program Leadership Roles	a. Appoint a Senior Accountable Official for Risk Management to align organizational information security and privacy management processes with strategic, operational, and budgetary planning processes; andb. Establish a Risk Executive (function) to view and analyze risk from an organization-wide perspective and ensure management of risk is consistent across the organization.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5		Not Associated
PM-29	Risk Management Program Leadership Roles	a. Appoint a Senior Accountable Official for Risk Management to align organizational information security and privacy management processes with strategic, operational, and budgetary planning processes; andb. Establish a Risk Executive (function) to view and analyze risk from an organization-wide perspective and ensure management of risk is consistent across the organization.	Functional	Intersects With	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	5		Not Associated
PM-30	Supply Chain Risk Management Strategy	a. Develop an organization-wide strategy for managing supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services;b. Implement the supply chain risk management strategy consistently across the organization; andc. Review and update the supply chain risk management strategy on [Assignment: organization-defined frequency] or as required, to address organizational changes.	Functional	Equal	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against	10		Not Associated
PM-30(01)	Supply Chain Risk Management Strategy | Suppliers of Critical or Mission-essential Items	Identify, prioritize, and assess suppliers of critical or mission-essential technologies, products, and services.	Functional	Intersects With	Customized Development of Critical Components	TDA-12	Mechanisms exist to custom-develop critical system components, when Commercial Off The Shelf (COTS) solutions are unavailable.	5		Not Associated
PM-30(01)	Supply Chain Risk Management Strategy | Suppliers of Critical or Mission-essential Items	Identify, prioritize, and assess suppliers of critical or mission-essential technologies, products, and services.	Functional	Intersects With	Criticality Analysis During Development	TDA-06.1	Mechanisms exist to require the developer of the Technology Asset, Application and/or Service (TAAS) to perform a criticality analysis at organization-defined decision points in the Secure Development Life Cycle (SDLC).	5		Not Associated
PM-30(01)	Supply Chain Risk Management Strategy | Suppliers of Critical or Mission-essential Items	Identify, prioritize, and assess suppliers of critical or mission-essential technologies, products, and services.	Functional	Intersects With	Third-Party Criticality Assessments	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the	5		Not Associated
PM-31	Continuous Monitoring Strategy	Develop an organization-wide continuous monitoring strategy and implement continuous monitoring programs that include:a. Establishing the following organization-wide metrics to be monitored: [Assignment: organization-defined metrics];b. Establishing [Assignment: organization-defined monitoring frequencies] and [Assignment: organization-defined assessment frequencies] for control effectiveness; c. Ongoing monitoring of organizationally-defined metrics in accordance with the continuous monitoring strategy;d. Correlation and analysis of information generated by control assessments and monitoring;e. Response actions to address results of the analysis of control assessment and monitoring information; andf. Reporting the security and privacy status of organizational systems to [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency].	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10		Not Associated
PM-32	Purposing	Analyze [Assignment: organization-defined systems or systems components] supporting mission essential services or functions to ensure that the information resources are being used consistent with their intended purpose.	Functional	Equal	Purpose Validation	GOV-11	Mechanisms exist to monitor mission/business-critical Technology Assets, Applications and/or Services (TAAS) to ensure those resources are being used consistent with their intended purpose.	10		Not Associated
PS-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] personnel security policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the personnel security policy and the associated personnel security controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the personnel security policy and procedures; andc. Review and update the current personnel security:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5		Low

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-53B Baseline
PS-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] personnel security policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the personnel security policy and the associated personnel security controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the personnel security policy and procedures; andc. Review and update the current personnel security:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5		Low
PS-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] personnel security policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the personnel security policy and the associated personnel security controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the personnel security policy and procedures; andc. Review and update the current personnel security:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10		Low
PS-02	Position Risk Designation	a. Assign a risk designation to all organizational positions;b. Establish screening criteria for individuals filling those positions; andc. Review and update position risk designations [Assignment: organization-defined frequency].	Functional	Intersects With	Competency Requirements for Security-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	5		Low
PS-02	Position Risk Designation	a. Assign a risk designation to all organizational positions;b. Establish screening criteria for individuals filling those positions; andc. Review and update position risk designations [Assignment: organization-defined frequency].	Functional	Intersects With	Position Categorization	HRS-02	Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions.	5		Low
PS-03	Personnel Screening	a. Screen individuals prior to authorizing access to the system; andb. Rescreen individuals in accordance with [Assignment: organization-defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of rescreening].	Functional	Equal	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	10		Low
PS-03(01)	Personnel Screening | Classified Information	Verify that individuals accessing a system processing, storing, or transmitting classified information are cleared and indoctrinated to the highest classification level of the information to which they have access on the system.	Functional	Intersects With	Roles With Special Protection Measures	HRS-04.1	Mechanisms exist to ensure that individuals accessing a system that stores, transmits or processes information requiring special protection satisfy organization-defined personnel screening criteria.	5		Not Selected
PS-03(02)	Personnel Screening | Formal Indoctrination	Verify that individuals accessing a system processing, storing, or transmitting types of classified information that require formal indoctrination, are formally indoctrinated for all the relevant types of information to which they have access on the system.	Functional	Equal	Formal Indoctrination	HRS-04.2	Mechanisms exist to formally educate authorized users on proper data handling practices for all the relevant types of data to which they have access.	10		Not Selected
PS-03(03)	Personnel Screening | Information Requiring Special Protective Measures	Verify that individuals accessing a system processing, storing, or transmitting information requiring special protection:a. Have valid access authorizations that are demonstrated by assigned official government duties; andb. Satisfy [Assignment: organization-defined additional personnel screening criteria].	Functional	Intersects With	Roles With Special Protection Measures	HRS-04.1	Mechanisms exist to ensure that individuals accessing a system that stores, transmits or processes information requiring special protection satisfy organization-defined personnel screening criteria.	5		Not Selected
PS-03(04)	Personnel Screening | Citizenship Requirements	Verify that individuals accessing a system processing, storing, or transmitting [Assignment: organization-defined information types] meet [Assignment: organization-defined citizenship requirements].	Functional	Equal	Citizenship Requirements	HRS-04.3	Mechanisms exist to verify that individuals accessing a system processing, storing, or transmitting sensitive information meet applicable statutory, regulatory and/or contractual requirements for citizenship.	10		Not Selected
PS-04	Personnel Termination	Upon termination of individual employment:a. Disable system access within [Assignment: organization-defined time period];b. Terminate or revoke any authenticators and credentials associated with the individual;c. Conduct exit interviews that include a discussion of [Assignment: organization-defined information security topics];d. Retrieve all security-related organizational system-related property; ande. Retain access to organizational information and systems formerly controlled by terminated individual.	Functional	Equal	Personnel Termination	HRS-09	Mechanisms exist to govern the termination of individual employment.	10		Low
PS-04(01)	Personnel Termination | Post-employment Requirements	a. Notify terminated individuals of applicable, legally binding post-employment requirements for the protection of organizational information; andb. Require terminated individuals to sign an acknowledgment of post-employment requirements as part of the organizational termination process.	Functional	Equal	Post-Employment Requirements Notification	HRS-09.3	Mechanisms exist to govern former employee behavior by formally notifying terminated individuals of their applicable, legally binding post-employment requirements for the protection of sensitive/regulated data.	10		Not Selected
PS-04(02)	Personnel Termination | Automated Actions	Use [Assignment: organization-defined automated mechanisms] to [Selection (one or more): notify [Assignment: organization-defined personnel or roles] of individual termination actions; disable access to system resources].	Functional	Equal	Automated Employment Status Notifications	HRS-09.4	Mechanisms exist to notify Identity and Access Management (IAM) personnel or roles upon termination of an individual employment or	10		High
PS-05	Personnel Transfer	a. Review and confirm ongoing operational need for current logical and physical access authorizations to systems and facilities when individuals are reassigned or transferred to other positions within the organization;b. Initiate [Assignment: organization-defined transfer or reassignment actions] within [Assignment: organization-defined time period following the formal transfer action];c. Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; andd. Notify [Assignment: organization-defined personnel or roles] within [Assignment:	Functional	Equal	Personnel Transfer	HRS-08	Mechanisms exist to adjust logical and physical access authorizations to Technology Assets, Applications and/or Services (TAAS) and facilities upon personnel reassignment or transfer, in a timely manner.	10		Low
PS-06	Access Agreements	a. Develop and document access agreements for organizational systems;b. Review and update the access agreements [Assignment: organization-defined frequency]; andc. Verify that individuals requiring access to organizational information and systems:1. Sign appropriate access agreements prior to being granted access; and2. Re-sign access agreements to maintain access to organizational systems when access agreements have been updated or [Assignment: organization-defined frequency].	Functional	Intersects With	Confidentiality Agreements	HRS-06.1	Mechanisms exist to require Non-Disclosure Agreements (NDAs) or similar confidentiality agreements that reflect the needs to protect data and operational details, or both employees and third-parties.	5		Low
PS-06	Access Agreements	a. Develop and document access agreements for organizational systems;b. Review and update the access agreements [Assignment: organization-defined frequency]; andc. Verify that individuals requiring access to organizational information and systems:1. Sign appropriate access agreements prior to being granted access; and2. Re-sign access agreements to maintain access to organizational systems when access agreements have been updated or [Assignment: organization-defined frequency].	Functional	Intersects With	Access Agreements	HRS-06	Mechanisms exist to require internal and third-party users to sign appropriate access agreements prior to being granted access.	5		Low
PS-06(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh	Notes	NIST SP 800-53B Baseline
PS-06(02)	Access Agreements | Classified Information Requiring Special Protection	Verify that access to classified information requiring special protection is granted only to individuals who:a. Have a valid access authorization that is demonstrated by assigned official government duties;b. Satisfy associated personnel security criteria; andc. Have read, understood, and signed a nondisclosure agreement.	Functional	Intersects With	Confidentiality Agreements	HRS-06.1	Mechanisms exist to require Non-Disclosure Agreements (NDAs) or similar confidentiality agreements that reflect the needs to protect data and operational details, or both employees and third-parties.	5		Not Selected
PS-06(02)	Access Agreements | Classified Information Requiring Special Protection	Verify that access to classified information requiring special protection is granted only to individuals who:a. Have a valid access authorization that is demonstrated by assigned official government duties;b. Satisfy associated personnel security criteria; andc. Have read, understood, and signed a nondisclosure agreement.	Functional	Intersects With	Access Agreements	HRS-06	Mechanisms exist to require internal and third-party users to sign appropriate access agreements prior to being granted access.	5		Not Selected
PS-06(03)	Access Agreements | Post-employment Requirements	a. Notify individuals of applicable, legally binding post-employment requirements for protection of organizational information; andb. Require individuals to sign an acknowledgment of these requirements, if applicable, as part of granting initial access to covered information.	Functional	Equal	Post-Employment Requirements Awareness	HRS-06.2	Mechanisms exist to notify individuals of their applicable, legally-binding post-employment requirements for the protection of sensitive/regulated data.	10		Not Selected
PS-07	External Personnel Security	a. Establish personnel security requirements, including security roles and responsibilities for external providers;b. Require external providers to comply with personnel security policies and procedures established by the organization;c. Document personnel security requirements;d. Require external providers to notify [Assignment: organization-defined personnel or roles] of any personnel transfers or terminations of external personnel who possess organizational credentials and/or badges, or who have system privileges within [Assignment: organization-defined time period]; ande. Monitor provider compliance with personnel security requirements.	Functional	Equal	Third-Party Personnel	HRS-10	Mechanisms exist to govern third-party personnel by reviewing and monitoring third-party security, compliance and/or resilience roles and responsibilities.	10		Low
PS-08	Personnel Sanctions	a. Employ a formal sanctions process for individuals failing to comply with established information security and privacy policies and procedures; andb. Notify [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period] when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.	Functional	Equal	Personnel Sanctions	HRS-07	Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.	10		Low
PS-09	Position Descriptions	Incorporate security and privacy roles and responsibilities into organizational position descriptions.	Functional	Equal	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	10		Low
PT-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] personally identifiable information processing and transparency policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the personally identifiable information processing and transparency policy and the associated personally identifiable information processing and transparency controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the personally identifiable information processing and transparency policy and procedures; andc. Review and update the current personally identifiable information processing and transparency:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5		Not Selected
PT-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] personally identifiable information processing and transparency policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the personally identifiable information processing and transparency policy and the associated personally identifiable information processing and transparency controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the personally identifiable information processing and transparency policy and procedures; andc. Review and update the current personally identifiable information processing and transparency:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5		Not Selected
PT-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] personally identifiable information processing and transparency policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the personally identifiable information processing and transparency policy and the associated personally identifiable information processing and transparency controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the personally identifiable information processing and transparency policy and procedures; andc. Review and update the current personally identifiable information processing and transparency:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Subset Of	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	10		Not Selected

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh	Notes	NIST SP 800-53B Baseline
PT-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] personally identifiable information processing and transparency policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the personally identifiable information processing and transparency policy and the associated personally identifiable information processing and transparency controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the personally identifiable information processing and transparency policy and procedures; andc. Review and update the current personally identifiable information processing and transparency:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	10		Not Selected
PT-02	Authority to Process Personally Identifiable Information	a. Determine and document the [Assignment: organization-defined authority] that permits the [Assignment: organization-defined processing] of personally identifiable information; andb. Restrict the [Assignment: organization-defined processing] of personally identifiable information to only that which is authorized.	Functional	Intersects With	Authority To Collect, Process, Store & Share Personal Data (PD)	PRI-04.1	Mechanisms exist to determine and document the legal authority that permits the organization to collect, receive, process, store, transmit, share, update and/or dispose Personal Data (PD), either generally or in support of a	5		Not Selected
PT-02	Authority to Process Personally Identifiable Information	a. Determine and document the [Assignment: organization-defined authority] that permits the [Assignment: organization-defined processing] of personally identifiable information; andb. Restrict the [Assignment: organization-defined processing] of personally identifiable information to only that which is authorized.	Functional	Intersects With	Internal Use of Personal Data (PD) For Testing, Training and Research	PRI-05.1	Mechanisms exist to address the use of Personal Data (PD) for internal testing, training and research that: (1) Takes measures to limit or minimize the amount of PD used for internal testing, training and research purposes; and (2) Authorizes the use of PD when such information is required for internal testing, training and research.	5		Not Selected
PT-02	Authority to Process Personally Identifiable Information	a. Determine and document the [Assignment: organization-defined authority] that permits the [Assignment: organization-defined processing] of personally identifiable information; andb. Restrict the [Assignment: organization-defined processing] of personally identifiable information to only that which is authorized.	Functional	Intersects With	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to: (1) The purpose(s) originally	5		Not Selected
PT-02	Authority to Process Personally Identifiable Information	a. Determine and document the [Assignment: organization-defined authority] that permits the [Assignment: organization-defined processing] of personally identifiable information; andb. Restrict the [Assignment: organization-defined processing] of personally identifiable information to only that which is authorized.	Functional	Intersects With	Restrict Collection To Identified Purpose	PRI-04	Mechanisms exist to minimize the collection of Personal Data (PD) to only what is adequate, relevant and limited to the purposes identified in the data privacy notice, including protections against collecting PD	5		Not Selected
PT-02(01)	Authority to Process Personally Identifiable Information | Data Tagging	Attach data tags containing [Assignment: organization-defined authorized processing] to [Assignment: organization-defined elements of personally identifiable information].	Functional	Equal	Data Tags	DCH-22.2	Mechanisms exist to utilize data tags to automate tracking of sensitive/regulated data across the information lifecycle.	10		Not Selected
PT-02(02)	Authority to Process Personally Identifiable Information | Automation	Manage enforcement of the authorized processing of personally identifiable information using [Assignment: organization-defined automated mechanisms].	Functional	Intersects With	Automated Data Management Processes	PRI-02.2	Automated mechanisms exist to adjust data that is able to be collected, received, processed, stored, transmitted, shared, updated and/or disposed, based on updated data subject authorization(s).	5		Not Selected
PT-03	Personally Identifiable Information Processing Purposes	a. Identify and document the [Assignment: organization-defined purpose(s)] for processing personally identifiable information;b. Describe the purpose(s) in the public privacy notices and policies of the organization;c. Restrict the [Assignment: organization-defined processing] of personally identifiable information to only that which is compatible with the identified purpose(s); andd. Monitor changes in processing personally identifiable information and implement [Assignment: organization-defined mechanisms] to ensure that any changes are made in accordance with [Assignment: organization-	Functional	Intersects With	Internal Use of Personal Data (PD) For Testing, Training and Research	PRI-05.1	Mechanisms exist to address the use of Personal Data (PD) for internal testing, training and research that: (1) Takes measures to limit or minimize the amount of PD used for internal testing, training and research purposes; and (2) Authorizes the use of PD when such information is required for internal testing, training and research.	5		Not Selected
PT-03	Personally Identifiable Information Processing Purposes	a. Identify and document the [Assignment: organization-defined purpose(s)] for processing personally identifiable information;b. Describe the purpose(s) in the public privacy notices and policies of the organization;c. Restrict the [Assignment: organization-defined processing] of personally identifiable information to only that which is compatible with the identified purpose(s); andd. Monitor changes in processing personally identifiable information and implement [Assignment: organization-defined mechanisms] to ensure that any changes are made in accordance with [Assignment: organization-	Functional	Intersects With	Purpose Specification	PRI-02.1	Mechanisms exist to ensure data privacy notices identify the purpose(s) for which Personal Data (PD) is collected, received, processed, stored, transmitted and/or shared.	5		Not Selected
PT-03(01)	Personally Identifiable Information Processing Purposes | Data Tagging	Attach data tags containing the following purposes to [Assignment: organization-defined elements of personally identifiable information]: [Assignment: organization-defined processing purposes].	Functional	Intersects With	Data Tagging	PRI-11	Mechanisms exist to issue data modeling guidelines to support tagging of sensitive/regulated data.	5		Not Selected
PT-03(01)	Personally Identifiable Information Processing Purposes | Data Tagging	Attach data tags containing the following purposes to [Assignment: organization-defined elements of personally identifiable information]: [Assignment: organization-defined processing purposes].	Functional	Intersects With	Data Tags	DCH-22.2	Mechanisms exist to utilize data tags to automate tracking of sensitive/regulated data across the information lifecycle.	5		Not Selected
PT-03(02)	Personally Identifiable Information Processing Purposes |	Track processing purposes of personally identifiable information using [Assignment: organization-defined automated mechanisms].	Functional	Intersects With	Data Quality Automation	PRI-10.1	Automated mechanisms exist to support the evaluation of data quality across the information lifecycle.	5		Not Selected
PT-03(02)	Personally Identifiable Information Processing Purposes | Automation	Track processing purposes of personally identifiable information using [Assignment: organization-defined automated mechanisms].	Functional	Intersects With	Automated Data Management Processes	PRI-02.2	Automated mechanisms exist to adjust data that is able to be collected, received, processed, stored, transmitted, shared, updated and/or disposed, based on updated data subject authorization(s).	5		Not Selected
PT-04	Consent	Implement [Assignment: organization-defined tools or mechanisms] for individuals to consent to the processing of their personally identifiable information prior to its collection that facilitate individuals' informed decision-making.	Functional	Equal	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (1) Plain language to illustrate	10		Not Selected
PT-04(01)	Consent | Tailored Consent	Provide [Assignment: organization-defined mechanisms] to allow individuals to tailor processing permissions to selected elements of personally identifiable information.	Functional	Equal	Tailored Consent	PRI-03.1	Mechanisms exist to allow data subjects to modify permission to collect, receive, process, store, transmit, share, update and/or	10		Not Selected
PT-04(02)	Consent | Just-in-time Consent	Present [Assignment: organization-defined consent mechanisms] to individuals at [Assignment: organization-defined frequency] and in conjunction with [Assignment: organization-defined personally identifiable information processing].	Functional	Intersects With	Just-In-Time Notice & Updated Consent	PRI-03.2	Mechanisms exist to present data subjects with a new or updated consent request to collect, receive, process, store, transmit, share, update and/or dispose Personal Data (PD) in conjunction with the data action, when: (1) The original circumstances under which an individual gave consent have changed; or (2) A significant amount of time	5		Not Selected
PT-04(03)	Consent | Revocation	Implement [Assignment: organization-defined tools or mechanisms] for individuals to revoke consent to the processing of their personally identifiable information.	Functional	Equal	Revoke Consent	PRI-03.4	Mechanisms exist to allow data subjects to revoke consent to collect, receive, process, store,	10		Not Selected

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh	Notes	NIST SP 800-53B Baseline
PT-05	Privacy Notice	Provide notice to individuals about the processing of personally identifiable information that:a. Is available to individuals upon first interacting with an organization, and subsequently at [Assignment: organization-defined frequency];b. Is clear and easy-to-understand, expressing information about personally identifiable information processing in plain language;c. Identifies the authority that authorizes the processing of personally identifiable information;d. Identifies the purposes for which personally identifiable information is to be processed; ande. Includes [Assignment: organization-defined information].	Functional	Intersects With	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations; (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and	5		Not Selected
PT-05(01)	Privacy Notice | Just-in-time Notice	Present notice of personally identifiable information processing to individuals at a time and location where the individual provides personally identifiable information or in conjunction with a data action, or [Assignment: organization-defined frequency].	Functional	Intersects With	Just-In-Time Notice & Updated Consent	PRI-03.2	Mechanisms exist to present data subjects with a new or updated consent request to collect, receive, process, store, transmit, share, update and/or dispose Personal Data (PD) in conjunction with the data action, when: (1) The original circumstances under which an individual gave consent have changed; or (2) A significant amount of time	5		Not Selected
PT-05(02)	Privacy Notice | Privacy Act Statements	Include Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.	Functional	Equal	Privacy Act Statements	PRI-01.2	Mechanisms exist to provide additional formal notice to individuals from whom the information is being collected that includes: (1) Notice of the authority of organizations to collect Personal Data (PD); (2) Whether providing PD is mandatory or optional; (3) The principal purpose or purposes for which the PD is to be used; (4) The intended disclosures or routine uses of the information; and (5) The consequences of not providing all or some portion of the information requested.	10		Not Selected
PT-06	System of Records Notice	For systems that process information that will be maintained in a Privacy Act system of records:a. Draft system of records notices in accordance with OMB guidance and submit new and significantly modified system of records notices to the OMB and appropriate congressional committees for advance review;b. Publish system of records notices in the Federal Register; andc. Keep system of records notices accurate, up-to-date, and scoped in accordance with policy.	Functional	Equal	System of Records Notice (SORN)	PRI-02.4	Mechanisms exist to draft, publish and keep System of Records Notices (SORN) updated in accordance with regulatory guidance.	10		Not Selected
PT-06(01)	System of Records Notice | Routine Uses	Review all routine uses published in the system of records notice at [Assignment: organization-defined frequency] to ensure continued accuracy, and to ensure that routine uses continue to be compatible with the purpose for which the information was collected.	Functional	Equal	System of Records Notice (SORN) Review Process	PRI-02.5	Mechanisms exist to review all routine uses of data published in the System of Records Notices (SORN) to ensure continued accuracy and to ensure that routine uses continue to be compatible with the purpose for which the information was collected.	10		Not Selected
PT-06(02)	System of Records Notice | Exemption Rules	Review all Privacy Act exemptions claimed for the system of records at [Assignment: organization-defined frequency] to ensure they remain appropriate and necessary in accordance with law, that they have been promulgated as regulations, and that they are accurately described in the system of records notice.	Functional	Equal	Privacy Act Exemptions	PRI-02.6	Mechanisms exist to review all Privacy Act exemptions claimed for the System of Records Notices (SORN) to ensure they remain appropriate and accurate.	10		Not Selected
PT-07	Specific Categories of Personally Identifiable Information	Apply [Assignment: organization-defined processing conditions] for specific categories of personally identifiable information.	Functional	Intersects With	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to: (1) The purpose(s) originally	5		Not Selected
PT-07	Specific Categories of Personally Identifiable Information	Apply [Assignment: organization-defined processing conditions] for specific categories of personally identifiable information.	Functional	Intersects With	Personal Data (PD) Categories	PRI-05.7	Mechanisms exist to define and implement data handling and protection requirements for specific categories of sensitive Personal Data (PD).	5		Not Selected
PT-07(01)	Specific Categories of Personally Identifiable Information | Social Security Numbers	When a system processes Social Security numbers:a. Eliminate unnecessary collection, maintenance, and use of Social Security numbers, and explore alternatives to their use as a personal identifier;b. Do not deny any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his or her Social Security number; andc. Inform any individual who is asked to disclose his or her Social Security number whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.	Functional	Intersects With	Personal Data (PD) Categories	PRI-05.7	Mechanisms exist to define and implement data handling and protection requirements for specific categories of sensitive Personal Data (PD).	5		Not Selected
PT-07(02)	Specific Categories of Personally Identifiable Information | First Amendment Information	Prohibit the processing of information describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual or unless pertinent to and within the scope of an authorized law enforcement activity.	Functional	Intersects With	Personal Data (PD) Categories	PRI-05.7	Mechanisms exist to define and implement data handling and protection requirements for specific categories of sensitive Personal Data (PD).	5		Not Selected
PT-08	Computer Matching Requirements	When a system or organization processes information for the purpose of conducting a matching program:a. Obtain approval from the Data Integrity Board to conduct the matching program;b. Develop and enter into a computer matching agreement;c. Publish a matching notice in the Federal Register;d. Independently verify the information produced by the matching program before taking adverse action against an individual, if required; ande. Provide individuals with notice and an opportunity to contest the findings before taking adverse action against an individual.	Functional	Intersects With	Computer Matching Agreements (CMA)	PRI-02.3	Mechanisms exist to publish Computer Matching Agreements (CMA) on the organization's public website(s).	5		Not Selected
RA-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] risk assessment policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the risk assessment policy and procedures; andc. Review and update the current risk assessment:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5		Low

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-53B Baseline
RA-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] risk assessment policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the risk assessment policy and procedures; andc. Review and update the current risk assessment:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10		Low
RA-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] risk assessment policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the risk assessment policy and procedures; andc. Review and update the current risk assessment:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5		Low
RA-02	Security Categorization	a. Categorize the system and information it processes, stores, and transmits;b. Document the security categorization results, including supporting rationale, in the security plan for the system; andc. Verify that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.	Functional	Equal	Risk-Based Security Categorization	RSK-02	Mechanisms exist to categorize Technology Assets, Applications, Services and/or Data (TAASD) in accordance with applicable laws, regulations and contractual obligations that: (1) Document the security categorization results (including supporting rationale) in the security plan for systems; and (2) Ensure the security categorization decision is reviewed and approved by the asset owner.	10		Low
RA-02(01)	Security Categorization | Impact-level Prioritization	Conduct an impact-level prioritization of organizational systems to obtain additional granularity on system impact levels.	Functional	Equal	Impact-Level Prioritization	RSK-02.1	Mechanisms exist to prioritize the impact level for Technology Assets, Applications and/or Services (TAAS) to prevent potential disruptions.	10		Not Selected
RA-03	Risk Assessment	a. Conduct a risk assessment, including:1. Identifying threats to and vulnerabilities in the system;2. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and3. Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information;b. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments;c. Document risk assessment results in [Selection (one): security and privacy plans; risk assessment report; [Assignment: organization-defined document]];d. Review risk assessment results [Assignment: organization-defined frequency];e. Disseminate risk assessment results to [Assignment: organization-defined personnel or roles]; andf. Update the risk assessment [Assignment: organization-defined frequency] or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.	Functional	Intersects With	Functional Review Of Security, Compliance & Resilience Controls	CPL-03.2	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's security, compliance and/or resilience policies and standards.	5		Low
RA-03	Risk Assessment	a. Conduct a risk assessment, including:1. Identifying threats to and vulnerabilities in the system;2. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and3. Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information;b. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments;c. Document risk assessment results in [Selection (one): security and privacy plans; risk assessment report; [Assignment: organization-defined document]];d. Review risk assessment results [Assignment: organization-defined frequency];e. Disseminate risk assessment results to [Assignment: organization-defined personnel or roles]; andf. Update the risk assessment [Assignment: organization-defined frequency] or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.	Functional	Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5		Low
RA-03(01)	Risk Assessment | Supply Chain Risk Assessment	a. Assess supply chain risks associated with [Assignment: organization-defined systems, system components, and system services]; andb. Update the supply chain risk assessment [Assignment: organization-defined frequency], when there are significant changes to the relevant supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in the supply chain.	Functional	Equal	Supply Chain Risk Assessment	RSK-09.1	Mechanisms exist to periodically assess supply chain risks associated with Technology Assets, Applications and/or Services (TAAS).	10		Low
RA-03(02)	Risk Assessment | Use of All-source Intelligence	Use all-source intelligence to assist in the analysis of risk.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
RA-03(03)	Risk Assessment | Dynamic Threat Awareness	Determine the current cyber threat environment on an ongoing basis using [Assignment: organization-defined means].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
RA-03(04)	Risk Assessment | Predictive Cyber Analytics	Employ the following advanced automation and analytics capabilities to predict and identify risks to [Assignment: organization-defined systems or system components]: [Assignment: organization-defined advanced automation and analytics capabilities].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
RA-04		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-53B Baseline
RA-05	Vulnerability Monitoring and Scanning	and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system are identified and reported;b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:1. Enumerating platforms, software flaws, and improper configurations;2. Formatting checklists and test procedures; and3. Measuring vulnerability impact;c. Analyze vulnerability scan reports and results from vulnerability monitoring;d. Remediate legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk;e. Share information obtained from the vulnerability monitoring process and control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other systems; andf. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5		Low
RA-05	Vulnerability Monitoring and Scanning	and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system are identified and reported;b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:1. Enumerating platforms, software flaws, and improper configurations;2. Formatting checklists and test procedures; and3. Measuring vulnerability impact;c. Analyze vulnerability scan reports and results from vulnerability monitoring;d. Remediate legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk;e. Share information obtained from the vulnerability monitoring process and control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other systems; andf. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be	Functional	Intersects With	Update Tool Capability	VPM-06.1	Mechanisms exist to update vulnerability scanning tools.	5		Low
RA-05(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
RA-05(02)	Vulnerability Monitoring and Scanning | Update Vulnerabilities to Be Scanned	Update the system vulnerabilities to be scanned [Selection (one or more): [Assignment: organization-defined frequency]; prior to a new scan; when new vulnerabilities are identified and reported].	Functional	Intersects With	Update Tool Capability	VPM-06.1	Mechanisms exist to update vulnerability scanning tools.	5		Low
RA-05(03)	Vulnerability Monitoring and Scanning | Breadth and Depth of Coverage	Define the breadth and depth of vulnerability scanning coverage.	Functional	Equal	Breadth / Depth of Coverage	VPM-06.2	Mechanisms exist to identify the breadth and depth of coverage for vulnerability scanning that define the system components scanned and types of vulnerabilities that are checked for.	10		Not Selected
RA-05(04)	Vulnerability Monitoring and Scanning | Discoverable Information	Determine information about the system that is discoverable and take [Assignment: organization-defined corrective actions].	Functional	Equal	Acceptable Discoverable Information	VPM-06.8	Mechanisms exist to define what information is allowed to be discoverable by adversaries and take corrective actions to remediate non-compliant Technology Assets, Applications	10		High
RA-05(05)	Vulnerability Monitoring and Scanning | Privileged Access	Implement privileged access authorization to [Assignment: organization-defined system components] for [Assignment: organization-defined vulnerability scanning activities].	Functional	Equal	Privileged Access	VPM-06.3	Mechanisms exist to implement privileged access authorization for selected vulnerability scanning activities.	10		Moderate
RA-05(06)	Vulnerability Monitoring and Scanning | Automated Trend Analyses	Compare the results of multiple vulnerability scans using [Assignment: organization-defined automated mechanisms].	Functional	Equal	Trend Analysis	VPM-06.4	Automated mechanisms exist to compare the results of vulnerability scans over time to determine trends in system vulnerabilities.	10		Not Selected
RA-05(07)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
RA-05(08)	Vulnerability Monitoring and Scanning | Review Historic Audit Logs	Review historic audit logs to determine if a vulnerability identified in a [Assignment: organization-defined system] has been previously exploited within an [Assignment: organization-defined time period].	Functional	Equal	Review Historical Event logs	VPM-06.5	Mechanisms exist to review historical event logs to determine if identified vulnerabilities have been previously exploited.	10		Not Selected
RA-05(09)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
RA-05(10)	Vulnerability Monitoring and Scanning | Correlate Scanning Information	Correlate the output from vulnerability scanning tools to determine the presence of multi-vulnerability and multi-hop attack vectors.	Functional	Equal	Correlate Scanning Information	VPM-06.9	Automated mechanisms exist to correlate the output from vulnerability scanning tools to determine the presence of multi-vulnerability/multi-hop attack vectors.	10		Not Selected
RA-05(11)	Vulnerability Monitoring and Scanning | Public Disclosure Program	Establish a public reporting channel for receiving reports of vulnerabilities in organizational systems and system components.	Functional	Equal	Vulnerability Disclosure Program (VDP)	THR-06	Mechanisms exist to establish a Vulnerability Disclosure Program (VDP) to assist with the secure development and maintenance of Technology Assets, Applications and/or Services (TAAS) that receives unsolicited input from the public about vulnerabilities in organizational	10		Low
RA-06	Technical Surveillance Countermeasures Survey	Employ a technical surveillance countermeasures survey at [Assignment: organization-defined locations] [Selection (one or more): [Assignment: organization-defined frequency]; when the following events or indicators occur: [Assignment: organization-defined events or indicators]].	Functional	Equal	Technical Surveillance Countermeasures Security	VPM-08	Mechanisms exist to utilize a technical surveillance countermeasures survey.	10		Not Selected
RA-07	Risk Response	Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.	Functional	Equal	Risk Response	RSK-06.1	proper risk response actions were performed to remediate findings from security, compliance and/or resilience-related: (1) Assessments;	10		Low
RA-08	Privacy Impact Assessments	Conduct privacy impact assessments for systems, programs, or other activities before:a. Developing or procuring information technology that processes personally identifiable information; andb. Initiating a new collection of personally identifiable information that:1. Will be processed using information technology; and2. Includes personally identifiable information permitting the physical or virtual (online) contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, ten or more individuals, other than agencies, instrumentalities, or employees of the federal government.	Functional	Equal	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10		Not Selected
RA-09	Criticality Analysis	Identify critical system components and functions by performing a criticality analysis for [Assignment: organization-defined systems, system components, or system services] at [Assignment: organization-defined decision points in the system development life cycle].	Functional	Intersects With	Third-Party Criticality Assessments	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the	5		Moderate
RA-09	Criticality Analysis	Identify critical system components and functions by performing a criticality analysis for [Assignment: organization-defined systems, system components, or system services] at [Assignment: organization-defined decision points in the system development life cycle].	Functional	Intersects With	Criticality Analysis During Development	TDA-06.1	Mechanisms exist to require the developer of the Technology Asset, Application and/or Service (TAAS) to perform a criticality analysis at organization-defined decision points in the Secure Development Life Cycle (SDLC).	5		Moderate
RA-09	Criticality Analysis	Identify critical system components and functions by performing a criticality analysis for [Assignment: organization-defined systems, system components, or system services] at [Assignment: organization-defined decision points in the system development life cycle].	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical Technology Assets, Applications and/or Services (TAAS) at pre-defined decision points in the Secure Development Life Cycle	5		Moderate

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh	Notes	NIST SP 800-53B Baseline
RA-10	Threat Hunting	a. Establish and maintain a cyber threat hunting capability to:1. Search for indicators of compromise in organizational systems; and2. Detect, track, and disrupt threats that evade existing controls; andb. Employ the threat hunting capability [Assignment: organization-defined frequency].	Functional	Equal	Threat Hunting	THR-07	Mechanisms exist to perform cyber threat hunting that uses Indicators of Compromise (IoC) to detect, track and disrupt threats that evade existing security controls.	10		Not Selected
SA-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and services acquisition policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the system and services acquisition policy and the associated system and services acquisition controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and services acquisition policy and procedures; andc. Review and update the current system and services acquisition:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5		Low
SA-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and services acquisition policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the system and services acquisition policy and the associated system and services acquisition controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and services acquisition policy and procedures; andc. Review and update the current system and services acquisition:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Subset Of	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	10		Low
SA-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and services acquisition policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the system and services acquisition policy and the associated system and services acquisition controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and services acquisition policy and procedures; andc. Review and update the current system and services acquisition:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5		Low
SA-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and services acquisition policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the system and services acquisition policy and the associated system and services acquisition controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and services acquisition policy and procedures; andc. Review and update the current system and services acquisition:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5		Low
SA-02	Allocation of Resources	a. Determine the high-level information security and privacy requirements for the system or system service in mission and business process planning;b. Determine, document, and allocate the resources required to protect the system or system service as part of the organizational capital planning and investment control process; andc. Establish a discrete line item for information security and privacy in organizational programming and budgeting documentation.	Functional	Equal	Allocation of Resources	PRM-03	Mechanisms exist to identify and allocate resources for management, operational, technical and data protection requirements within business process planning for projects / initiatives.	10		Low
SA-03	System Development Life Cycle	a. Acquire, develop, and manage the system using [Assignment: organization-defined system development life cycle] that incorporates information security and privacy considerations;b. Define and document information security and privacy roles and responsibilities throughout the system development life cycle;c. Identify individuals having information security and privacy roles and responsibilities; andd. Integrate the organizational information security and privacy risk management process into system development life cycle activities.	Functional	Intersects With	Technology Lifecycle Management	SEA-07.1	Mechanisms exist to manage the usable lifecycles of Technology Assets, Applications and/or Services (TAAS).	5		Low
SA-03	System Development Life Cycle	a. Acquire, develop, and manage the system using [Assignment: organization-defined system development life cycle] that incorporates information security and privacy considerations;b. Define and document information security and privacy roles and responsibilities throughout the system development life cycle;c. Identify individuals having information security and privacy roles and responsibilities; andd. Integrate the organizational information security and privacy risk management process into system development life cycle activities.	Functional	Intersects With	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5		Low
SA-03(01)	System Development Life Cycle | Manage Preproduction Environment	Protect system preproduction environments commensurate with risk throughout the system development life cycle for the system, system component, or system service.	Functional	Intersects With	Technology Lifecycle Management	SEA-07.1	Mechanisms exist to manage the usable lifecycles of Technology Assets, Applications and/or Services (TAAS).	5		Not Selected
SA-03(01)	System Development Life Cycle | Manage Preproduction Environment	Protect system preproduction environments commensurate with risk throughout the system development life cycle for the system, system component, or system service.	Functional	Intersects With	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5		Not Selected
SA-03(01)	System Development Life Cycle | Manage Preproduction Environment	Protect system preproduction environments commensurate with risk throughout the system development life cycle for the system, system component, or system service.	Functional	Intersects With	Secure Development Environments	TDA-07	Mechanisms exist to maintain a segmented development network to ensure a secure development environment.	5		Not Selected

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-53B Baseline
SA-03(02)	System Development Life Cycle | Use of Live or Operational Data	a. Approve, document, and control the use of live data in preproduction environments for the system, system component, or system service; andb. Protect preproduction environments for the system, system component, or system service at the same impact or classification level as any live data in use within the preproduction environments.	Functional	Equal	Use of Live Data	TDA-10	Mechanisms exist to approve, document and control the use of live data in development and test environments.	10		Not Selected
SA-03(03)	System Development Life Cycle | Technology Refresh	Plan for and implement a technology refresh schedule for the system throughout the system development life cycle.	Functional	Intersects With	Technology Lifecycle Management	SEA-07.1	Mechanisms exist to manage the usable lifecycles of Technology Assets, Applications and/or Services (TAAS).	5		Not Selected
SA-03(03)	System Development Life Cycle | Technology Refresh	Plan for and implement a technology refresh schedule for the system throughout the system development life cycle.	Functional	Intersects With	Refresh from Trusted Sources	SEA-08.1	Mechanisms exist to ensure that software and data needed for system component and service refreshes are obtained from trusted sources.	5		Not Selected
SA-04	Acquisition Process	Include the following requirements, descriptions, and criteria, explicitly or by reference, using [Selection (one or more): standardized contract language; [Assignment: organization-defined contract language]] in the acquisition contract for the system, system component, or system service:a. Security and privacy functional requirements;b. Strength of mechanism requirements;c. Security and privacy assurance requirements;d. Controls needed to satisfy the security and privacy requirements.e. Security and privacy documentation requirements;f. Requirements for protecting security and privacy documentation;g. Description of the system development environment and environment in which the system is intended to operate;h. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; andi. Acceptance criteria.	Functional	Intersects With	Minimum Viable Product (MVP) Security Requirements	TDA-02	Mechanisms exist to design, develop and produce Technology Assets, Applications and/or Services (TAAS) in such a way that risk-based technical and functional specifications ensure Minimum Viable Product (MVP) criteria establish an appropriate level of security and resiliency based on applicable risks and threats.	5		Low
SA-04	Acquisition Process	Include the following requirements, descriptions, and criteria, explicitly or by reference, using [Selection (one or more): standardized contract language; [Assignment: organization-defined contract language]] in the acquisition contract for the system, system component, or system service:a. Security and privacy functional requirements;b. Strength of mechanism requirements;c. Security and privacy assurance requirements;d. Controls needed to satisfy the security and privacy requirements.e. Security and privacy documentation requirements;f. Requirements for protecting security and privacy documentation;g. Description of the system development environment and environment in which the system is intended to operate;h. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; andi. Acceptance criteria.	Functional	Intersects With	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5		Low
SA-04	Acquisition Process	Include the following requirements, descriptions, and criteria, explicitly or by reference, using [Selection (one or more): standardized contract language; [Assignment: organization-defined contract language]] in the acquisition contract for the system, system component, or system service:a. Security and privacy functional requirements;b. Strength of mechanism requirements;c. Security and privacy assurance requirements;d. Controls needed to satisfy the security and privacy requirements.e. Security and privacy documentation requirements;f. Requirements for protecting security and privacy documentation;g. Description of the system development environment and environment in which the system is intended to operate;h. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; andi. Acceptance criteria.	Functional	Intersects With	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	5		Low
SA-04	Acquisition Process	Include the following requirements, descriptions, and criteria, explicitly or by reference, using [Selection (one or more): standardized contract language; [Assignment: organization-defined contract language]] in the acquisition contract for the system, system component, or system service:a. Security and privacy functional requirements;b. Strength of mechanism requirements;c. Security and privacy assurance requirements;d. Controls needed to satisfy the security and privacy requirements.e. Security and privacy documentation requirements;f. Requirements for protecting security and privacy documentation;g. Description of the system development environment and environment in which the system is intended to operate;h. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; andi. Acceptance criteria.	Functional	Intersects With	Managing Changes To Third-Party Services	TPM-10	Mechanisms exist to control changes to services by suppliers, taking into account the criticality of business Technology Assets, Applications, Services and/or Data (TAASD) that are in scope by the third-party.	5		Low
SA-04(01)	Acquisition Process | Functional Properties of Controls	Require the developer of the system, system component, or system service to provide a description of the functional properties of the controls to be implemented.	Functional	Intersects With	Functional Properties	TDA-04.1	Mechanisms exist to require software developers to provide information describing the functional properties of the security, compliance and resilience controls to be utilized within Technology Assets, Applications and/or Services (TAAS) in sufficient detail to	5		Moderate
SA-04(01)	Acquisition Process | Functional Properties of Controls	Require the developer of the system, system component, or system service to provide a description of the functional properties of the controls to be implemented.	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive/regulated data flows.	5		Moderate
SA-04(02)	Acquisition Process | Design and Implementation Information for Controls	Require the developer of the system, system component, or system service to provide design and implementation information for the controls that includes: [Selection (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; [Assignment: organization-defined design and implementation information]] at [Assignment: organization-defined level of detail].	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive/regulated data flows.	5		Moderate
SA-04(02)	Acquisition Process | Design and Implementation Information for Controls	Require the developer of the system, system component, or system service to provide design and implementation information for the controls that includes: [Selection (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; [Assignment: organization-defined design and implementation information]] at [Assignment: organization-defined level of detail].	Functional	Intersects With	Access to Program Source Code	TDA-20	Mechanisms exist to limit privileges to change software resident within software libraries.	5		Moderate
SA-04(02)	Acquisition Process | Design and Implementation Information for Controls	Require the developer of the system, system component, or system service to provide design and implementation information for the controls that includes: [Selection (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; [Assignment: organization-defined design and implementation information]] at [Assignment: organization-defined level of detail].	Functional	Intersects With	Functional Properties	TDA-04.1	Mechanisms exist to require software developers to provide information describing the functional properties of the security, compliance and resilience controls to be utilized within Technology Assets, Applications and/or Services (TAAS) in sufficient detail to	5		Moderate
SA-04(03)	Acquisition Process | Development Methods, Techniques, and Practices	Require the developer of the system, system component, or system service to demonstrate the use of a system development life cycle process that includes:a. [Assignment: organization-defined systems engineering methods];b. [Assignment: organization-defined [Selection (one or more): systems security; privacy] engineering methods]; andc. [Assignment: organization-defined software development methods; testing, evaluation, assessment, verification, and validation methods; and quality control processes].	Functional	Intersects With	Development Methods, Techniques & Processes	TDA-02.3	Mechanisms exist to require software developers to ensure that their software development processes employ industry-recognized secure practices for secure programming, engineering methods, quality control processes and validation techniques to minimize flawed and/or malformed software.	5		Not Selected

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-53B Baseline
SA-04(03)	Acquisition Process | Development Methods, Techniques, and Practices	Require the developer of the system, system component, or system service to demonstrate the use of a system development life cycle process that includes:a. [Assignment: organization-defined systems engineering methods];b. [Assignment: organization-defined [Selection (one or more): systems security; privacy] engineering methods]; andc. [Assignment: organization-defined software development methods; testing, evaluation, assessment, verification, and validation methods; and quality control processes].	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5		Not Selected
SA-04(04)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SA-04(05)	Acquisition Process | System, Component, and Service Configurations	Require the developer of the system, system component, or system service to:a. Deliver the system, component, or service with [Assignment: organization-defined security configurations] implemented; andb. Use the configurations as the default for any subsequent system, component, or service reinstallation or upgrade.	Functional	Equal	Pre-Established Secure Configurations	TDA-02.4	Mechanisms exist to ensure vendors / manufacturers: (1) Deliver the Technology Asset, Application and/or Service (TAAS) with a pre-established, secure configuration implemented; and (2) Use the pre-established, secure configuration as the default for any subsequent TAAS reinstallation or upgrade.	10		High
SA-04(06)	Acquisition Process | Use of Information Assurance Products	a. Employ only government off-the-shelf or commercial off-the-shelf information assurance and information assurance-enabled information technology products that compose an NSA-approved solution to protect classified information when the networks used to transmit the information are at a lower classification level than the information being transmitted; andb. Ensure that these products have been evaluated and/or validated by NSA or in accordance with NSA-approved procedures.	Functional	Equal	Commercial Off-The-Shelf (COTS) Security Solutions	TDA-03	Mechanisms exist to utilize only Commercial Off-the-Shelf (COTS) security products.	10		Not Selected
SA-04(07)	Acquisition Process | NIAP-approved Protection Profiles	a. Limit the use of commercially provided information assurance and information assurance-enabled information technology products to those products that have been successfully evaluated against a National Information Assurance partnership (NIAP)-approved Protection Profile for a specific technology type, if such a profile exists; andb. Require, if no NIAP-approved Protection Profile exists for a specific technology type but a commercially provided information technology product relies on cryptographic functionality to enforce its security policy, that the cryptographic module is FIPS-validated or NSA-approved.	Functional	Intersects With	Information Assurance Enabled Products	TDA-02.2	Mechanisms exist to limit the use of commercially-provided Information Assurance (IA) and IA-enabled IT products to those products that have been successfully evaluated against a National Information Assurance partnership (NIAP)-approved Protection Profile or the cryptographic module is FIPS-validated or NSA-approved.	5		Not Selected
SA-04(08)	Acquisition Process | Continuous Monitoring Plan for Controls	Require the developer of the system, system component, or system service to produce a plan for continuous monitoring of control effectiveness that is consistent with the continuous monitoring program of the organization.	Functional	Equal	Continuous Monitoring Plan	TDA-09.1	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to produce a plan for the continuous monitoring of security, compliance and/or resilience control effectiveness.	10		Not Selected
SA-04(09)	Acquisition Process | Functions, Ports, Protocols, and Services in Use	Require the developer of the system, system component, or system service to identify the functions, ports, protocols, and services intended for organizational use.	Functional	Equal	Ports, Protocols & Services In Use	TDA-02.1	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to identify early in the Secure Development Life Cycle (SDLC), the functions, ports, protocols and services intended for use.	10		Moderate
SA-04(10)	Acquisition Process | Use of Approved PIV Products	Employ only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational systems.	Functional	Intersects With	Information Assurance Enabled Products	TDA-02.2	Mechanisms exist to limit the use of commercially-provided Information Assurance (IA) and IA-enabled IT products to those products that have been successfully evaluated against a National Information Assurance partnership (NIAP)-approved Protection Profile or the cryptographic module is FIPS-validated or NSA-approved.	5		Low
SA-04(11)	Acquisition Process | System of Records	Include [Assignment: organization-defined Privacy Act requirements] in the acquisition contract for the operation of a system of records on behalf of an organization to accomplish an organizational mission or function.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SA-04(12)	Acquisition Process | Data Ownership	a. Include organizational data ownership requirements in the acquisition contract; andb. Require all data to be removed from the contractor's system and returned to the organization within [Assignment: organization-defined time frame].	Functional	Intersects With	Personal Data (PD) Lineage	PRI-09	Mechanisms exist to maintain a process to document the lineage of Personal Data (PD) by recording how the organization collects, receives, processes, stores, transmits, shares,	5		Not Selected
SA-04(12)	Acquisition Process | Data Ownership	a. Include organizational data ownership requirements in the acquisition contract; andb. Require all data to be removed from the contractor's system and returned to the organization within [Assignment: organization-defined time frame].	Functional	Intersects With	Data Stewardship	DCH-01.1	Mechanisms exist to ensure data stewardship is assigned, documented and communicated.	5		Not Selected
SA-04(12)	Acquisition Process | Data Ownership	a. Include organizational data ownership requirements in the acquisition contract; andb. Require all data to be removed from the contractor's system and returned to the organization within [Assignment: organization-defined time frame].	Functional	Intersects With	Asset Ownership Assignment	AST-03	Mechanisms exist to ensure asset ownership responsibilities are assigned, tracked and managed at a team, individual, or responsible organization level to establish a common understanding of requirements for asset protection.	5		Not Selected
SA-05	System Documentation	a. Obtain or develop administrator documentation for the system, system component, or system service that describes:1. Secure configuration, installation, and operation of the system, component, or service;2. Effective use and maintenance of security and privacy functions and mechanisms; and3. Known vulnerabilities regarding configuration and use of administrative or privileged functions;b. Obtain or develop user documentation for the system, system component, or system service that describes:1. User-accessible security and privacy functions and mechanisms and how to effectively use those functions and mechanisms;2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner and protect individual privacy; and3. User responsibilities in maintaining the security of the system, component, or service and privacy of individuals;c. Document attempts to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent and take [Assignment: organization-defined actions] in response; andd. Distribute documentation to [Assignment: organization-defined personnel or roles].	Functional	Intersects With	Documentation Requirements	TDA-04	Mechanisms exist to obtain, protect and distribute administrator documentation for Technology Assets, Applications and/or Services (TAAS) that describe: (1) Secure configuration, installation and operation of the TAAS; (2) Effective use and maintenance of security features/functions; and (3) Known vulnerabilities regarding configuration and use of administrative (e.g., privileged) functions.	5		Low
SA-05	System Documentation	a. Obtain or develop administrator documentation for the system, system component, or system service that describes:1. Secure configuration, installation, and operation of the system, component, or service;2. Effective use and maintenance of security and privacy functions and mechanisms; and3. Known vulnerabilities regarding configuration and use of administrative or privileged functions;b. Obtain or develop user documentation for the system, system component, or system service that describes:1. User-accessible security and privacy functions and mechanisms and how to effectively use those functions and mechanisms;2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner and protect individual privacy; and3. User responsibilities in maintaining the security of the system, component, or service and privacy of individuals;c. Document attempts to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent and take [Assignment: organization-defined actions] in response; andd. Distribute documentation to [Assignment: organization-defined personnel or roles].	Functional	Intersects With	Asset Scope Classification	AST-04.1	Mechanisms exist to determine security, compliance and resilience control applicability by identifying, assigning and documenting the appropriate asset scope categorization for all Technology Assets, Applications and/or Services (TAAS) and personnel (internal and third-parties).	5		Low
SA-05(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SA-05(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-53B Baseline
SA-05(03)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SA-05(04)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SA-05(05)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SA-06		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SA-07		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SA-08	Security and Privacy Engineering Principles	Apply the following systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components: [Assignment: organization-defined systems security and privacy engineering principles].	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening	5		Low
SA-08	Security and Privacy Engineering Principles	Apply the following systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components: [Assignment: organization-defined systems security and privacy engineering principles].	Functional	Intersects With	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or	5		Low
SA-08(01)	Security and Privacy Engineering Principles | Clear Abstractions	Implement the security design principle of clear abstractions.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SA-08(02)	Security and Privacy Engineering Principles | Least Common Mechanism	Implement the security design principle of least common mechanism in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SA-08(03)	Security and Privacy Engineering Principles | Modularity and Layering	Implement the security design principles of modularity and layering in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SA-08(04)	Security and Privacy Engineering Principles | Partially Ordered Dependencies	Implement the security design principle of partially ordered dependencies in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SA-08(05)	Security and Privacy Engineering Principles | Efficiently Mediated Access	Implement the security design principle of efficiently mediated access in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SA-08(06)	Security and Privacy Engineering Principles | Minimized Sharing	Implement the security design principle of minimized sharing in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SA-08(07)	Security and Privacy Engineering Principles | Reduced Complexity	Implement the security design principle of reduced complexity in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SA-08(08)	Security and Privacy Engineering Principles | Secure Evolvability	Implement the security design principle of secure evolvability in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SA-08(09)	Security and Privacy Engineering Principles | Trusted Components	Implement the security design principle of trusted components in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SA-08(10)	Security and Privacy Engineering Principles | Hierarchical Trust	Implement the security design principle of hierarchical trust in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SA-08(11)	Security and Privacy Engineering Principles | Inverse Modification Threshold	Implement the security design principle of inverse modification threshold in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SA-08(12)	Privacy Engineering Principles | Hierarchical	Implement the security design principle of hierarchical protection in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SA-08(13)	Security and Privacy Engineering Principles | Minimized Security Elements	Implement the security design principle of minimized security elements in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SA-08(14)	Security and Privacy Engineering Principles | Least Privilege	Implement the security design principle of least privilege in [Assignment: organization-defined systems or system components].	Functional	Equal	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	10		Not Selected
SA-08(15)	Privacy Engineering Principles | Predicate	Implement the security design principle of predicate permission in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SA-08(16)	Security and Privacy Engineering Principles | Self-reliant Trustworthiness	Implement the security design principle of self-reliant trustworthiness in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SA-08(17)	Security and Privacy Engineering Principles | Secure Distributed Composition	Implement the security design principle of secure distributed composition in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SA-08(18)	Security and Privacy Engineering Principles | Trusted Communications Channels	Implement the security design principle of trusted communications channels in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SA-08(19)	Privacy Engineering Principles | Continuous	Implement the security design principle of continuous protection in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SA-08(20)	Security and Privacy Engineering Principles | Secure Metadata Management	Implement the security design principle of secure metadata management in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SA-08(21)	Security and Privacy Engineering Principles | Self-analysis	Implement the security design principle of self-analysis in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SA-08(22)	Security and Privacy Engineering Principles | Accountability and Traceability	Implement the security design principle of accountability and traceability in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SA-08(23)	Security and Privacy Engineering Principles | Secure Defaults	Implement the security design principle of secure defaults in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SA-08(24)	Security and Privacy Engineering Principles | Secure Failure and Recovery	Implement the security design principle of secure failure and recovery in [Assignment: organization-defined systems or system components].	Functional	Equal	Fail Secure	SEA-07.2	systems to fail to an organization-defined known-state for types of failures, preserving system state information in	10		Not Selected
SA-08(25)	Security and Privacy Engineering Principles | Economic Security	Implement the security design principle of economic security in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SA-08(26)	Privacy Engineering Principles | Performance	Implement the security design principle of performance security in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SA-08(27)	Security and Privacy Engineering Principles | Human Factored Security	Implement the security design principle of human factored security in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SA-08(28)	Security and Privacy Engineering Principles | Acceptable Security	Implement the security design principle of acceptable security in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-53B Baseline
SA-08(29)	Security and Privacy Engineering Principles | Repeatable and Documented Procedures	Implement the security design principle of repeatable and documented procedures in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SA-08(30)	Security and Privacy Engineering Principles | Procedural Rigor	Implement the security design principle of procedural rigor in [Assignment: organization-defined systems or system components].	Functional	Intersects With	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5		Not Selected
SA-08(30)	Security and Privacy Engineering Principles | Procedural Rigor	Implement the security design principle of procedural rigor in [Assignment: organization-defined systems or system components].	Functional	Intersects With	Technology Lifecycle Management	SEA-07.1	Mechanisms exist to manage the usable lifecycles of Technology Assets, Applications and/or Services (TAAS).	5		Not Selected
SA-08(31)	Security and Privacy Engineering Principles | Secure System Modification	Implement the security design principle of secure system modification in [Assignment: organization-defined systems or system components].	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5		Not Selected
SA-08(31)	Security and Privacy Engineering Principles | Secure System Modification	Implement the security design principle of secure system modification in [Assignment: organization-defined systems or system components].	Functional	Intersects With	Control Functionality Verification	CHG-06	Mechanisms exist to verify the functionality of security, compliance and resilience controls following implemented changes to ensure applicable controls operate as designed.	5		Not Selected
SA-08(31)	Security and Privacy Engineering Principles | Secure System Modification	Implement the security design principle of secure system modification in [Assignment: organization-defined systems or system components].	Functional	Intersects With	Test, Validate & Document Changes	CHG-02.2	Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented in a production environment.	5		Not Selected
SA-08(32)	Security and Privacy Engineering Principles | Sufficient Documentation	Implement the security design principle of sufficient documentation in [Assignment: organization-defined systems or system components].	Functional	Equal	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	10		Not Selected
SA-08(33)	Security and Privacy Engineering Principles | Minimization	Implement the privacy principle of minimization using [Assignment: organization-defined processes].	Functional	Intersects With	Collection Minimization	END-13.3	Mechanisms exist to utilize sensors that are configured to minimize the collection of information about individuals.	5		Not Selected
SA-08(33)	Security and Privacy Engineering Principles | Minimization	Implement the privacy principle of minimization using [Assignment: organization-defined processes].	Functional	Intersects With	Limit Sensitive / Regulated Data In Testing, Training & Research	DCH-18.2	Mechanisms exist to minimize the use of sensitive/regulated data for research, testing, or training, in accordance with authorized, legitimate business practices.	5		Not Selected
SA-08(33)	Security and Privacy Engineering Principles | Minimization	Implement the privacy principle of minimization using [Assignment: organization-defined processes].	Functional	Intersects With	Minimize Visitor Personal Data (PD)	PES-06.5	Mechanisms exist to minimize the collection of Personal Data (PD) contained in visitor access records.	5		Not Selected
SA-09	External System Services	a. Require that providers of external system services comply with organizational security and privacy requirements and employ the following controls: [Assignment: organization-defined controls];b. Define and document organizational oversight and user roles and responsibilities with regard to external system services; andc. Employ the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis: [Assignment: organization-defined processes, methods, and techniques].	Functional	Equal	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	10		Low
SA-09(01)	External System Services | Risk Assessments and Organizational Approvals	a. Conduct an organizational assessment of risk prior to the acquisition or outsourcing of information security services; andb. Verify that the acquisition or outsourcing of dedicated information security services is approved by [Assignment: organization-defined personnel or roles].	Functional	Equal	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	10		Not Selected
SA-09(02)	External System Services | Identification of Functions, Ports, Protocols, and Services	Require providers of the following external system services to identify the functions, ports, protocols, and other services required for the use of such services: [Assignment: organization-defined external system services].	Functional	Equal	External Connectivity Requirements - Identification of Ports, Protocols & Services	TPM-04.2	Mechanisms exist to require External Service Providers (ESPs) to identify and document the business need for ports, protocols and other services it requires to operate its Technology Assets, Applications	10		Moderate
SA-09(03)	External System Services | Establish and Maintain Trust Relationship with Providers	Establish, document, and maintain trust relationships with external service providers based on the following requirements, properties, factors, or conditions: [Assignment: organization-defined security and privacy requirements, properties, factors, or conditions defining acceptable trust relationships].	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5		Not Selected
SA-09(03)	External System Services | Establish and Maintain Trust Relationship with Providers	Establish, document, and maintain trust relationships with external service providers based on the following requirements, properties, factors, or conditions: [Assignment: organization-defined security and privacy requirements, properties, factors, or conditions defining acceptable trust relationships].	Functional	Intersects With	Conflict of Interests	TPM-04.3	Mechanisms exist to ensure that the interests of external service providers are consistent with and reflect organizational interests.	5		Not Selected
SA-09(03)	External System Services | Establish and Maintain Trust Relationship with Providers	Establish, document, and maintain trust relationships with external service providers based on the following requirements, properties, factors, or conditions: [Assignment: organization-defined security and privacy requirements, properties, factors, or conditions defining acceptable trust relationships].	Functional	Intersects With	Third-Party Criticality Assessments	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the	5		Not Selected
SA-09(03)	External System Services | Establish and Maintain Trust Relationship with Providers	Establish, document, and maintain trust relationships with external service providers based on the following requirements, properties, factors, or conditions: [Assignment: organization-defined security and privacy requirements, properties, factors, or conditions defining acceptable trust relationships].	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and (2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	5		Not Selected
SA-09(03)	External System Services | Establish and Maintain Trust Relationship with Providers	Establish, document, and maintain trust relationships with external service providers based on the following requirements, properties, factors, or conditions: [Assignment: organization-defined security and privacy requirements, properties, factors, or conditions defining acceptable trust relationships].	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for security, compliance and resilience controls between internal stakeholders and External Service Providers (ESPs).	5		Not Selected
SA-09(03)	External System Services | Establish and Maintain Trust Relationship with Providers	Establish, document, and maintain trust relationships with external service providers based on the following requirements, properties, factors, or conditions: [Assignment: organization-defined security and privacy requirements, properties, factors, or conditions defining acceptable trust relationships].	Functional	Intersects With	Break Clauses	TPM-05.7	Mechanisms exist to include "break clauses" within contracts for failure to meet contract criteria for security, compliance and/or resilience controls.	5		Not Selected
SA-09(04)	External System Services | Consistent Interests of Consumers and Providers	Take the following actions to verify that the interests of [Assignment: organization-defined external service providers] are consistent with and reflect organizational interests: [Assignment: organization-defined actions].	Functional	Equal	Conflict of Interests	TPM-04.3	Mechanisms exist to ensure that the interests of external service providers are consistent with and reflect organizational interests.	10		Not Selected
SA-09(05)	External System Services | Processing, Storage, and Service Location	Restrict the location of [Selection (one or more): information processing; information or data; system services] to [Assignment: organization-defined locations] based on [Assignment: organization-defined requirements or conditions].	Functional	Intersects With	Geolocation Requirements for Processing, Storage and Service Locations	CLD-09	Mechanisms exist to control the location of cloud processing/storage based on business requirements that includes statutory, regulatory and contractual obligations.	5		Not Selected
SA-09(05)	External System Services | Processing, Storage, and Service Location	Restrict the location of [Selection (one or more): information processing; information or data; system services] to [Assignment: organization-defined locations] based on [Assignment: organization-defined requirements or conditions].	Functional	Intersects With	Third-Party Processing, Storage and Service Locations	TPM-04.4	Mechanisms exist to restrict the location of information processing/storage based on business requirements.	5		Not Selected

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh	Notes	NIST SP 800-53B Baseline
SA-09(05)	External System Services | Processing, Storage, and Service Location	Restrict the location of [Selection (one or more): information processing; information or data; system services] to [Assignment: organization-defined locations] based on [Assignment: organization-defined requirements or conditions].	Functional	Intersects With	Geographic Location of Data	DCH-19	Mechanisms exist to inventory, document and maintain data flows for data that is resident (permanently or temporarily) within a service's geographically distributed applications (physical and virtual), infrastructure, systems components and/or shared with other third-parties.	5		Not Selected
SA-09(06)	External System Services | Organization-controlled Cryptographic Keys	Maintain exclusive control of cryptographic keys for encrypted material stored or transmitted through an external system.	Functional	Equal	External System Cryptographic Key Control	CRY-09.7	Mechanisms exist to maintain control of cryptographic keys for encrypted material stored or transmitted through an external system.	10		Not Selected
SA-09(07)	External System Services | Organization-controlled Integrity Checking	Provide the capability to check the integrity of information while it resides in the external system.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SA-09(08)	External System Services | Processing and Storage Location — U.S. Jurisdiction	Restrict the geographic location of information processing and data storage to facilities located within in the legal jurisdictional boundary of the United States.	Functional	Intersects With	Geographic Location of Data	DCH-19	Mechanisms exist to inventory, document and maintain data flows for data that is resident (permanently or temporarily) within a service's geographically distributed applications (physical and virtual), infrastructure, systems components and/or shared with other third-parties.	5		Not Selected
SA-09(08)	External System Services | Processing and Storage Location — U.S. Jurisdiction	Restrict the geographic location of information processing and data storage to facilities located within in the legal jurisdictional boundary of the United States.	Functional	Intersects With	Geolocation Requirements for Processing, Storage and Service Locations	CLD-09	Mechanisms exist to control the location of cloud processing/storage based on business requirements that includes statutory, regulatory and contractual obligations.	5		Not Selected
SA-10	Developer Configuration Management	Require the developer of the system, system component, or system service to:a. Perform configuration management during system, component, or service [Selection (one or more): design; development; implementation; operation; disposal];b. Document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items under configuration management];c. Implement only organization-approved changes to the system, component, or service;d. Document approved changes to the system, component, or service and the potential security and privacy impacts of such changes; ande. Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel].	Functional	Equal	Developer Configuration Management	TDA-14	Mechanisms exist to require system developers and integrators to perform configuration management during system design, development, implementation and operation.	10		Moderate
SA-10(01)	Developer Configuration Management | Software and Firmware Integrity Verification	Require the developer of the system, system component, or system service to enable integrity verification of software and firmware components.	Functional	Equal	Software / Firmware Integrity Verification	TDA-14.1	Mechanisms exist to require developers of Technology Assets, Applications and/or Services (TAAS) to enable integrity verification of software and firmware components.	10		Not Selected
SA-10(02)	Developer Configuration Management | Alternative Configuration Management Processes	Provide an alternate configuration management process using organizational personnel in the absence of a dedicated developer configuration management team.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SA-10(03)	Developer Configuration Management | Hardware Integrity Verification	Require the developer of the system, system component, or system service to enable integrity verification of hardware components.	Functional	Equal	Hardware Integrity Verification	TDA-14.2	Mechanisms exist to require developers of Technology Assets, Applications and/or Services (TAAS) to enable integrity verification of hardware components.	10		Not Selected
SA-10(04)	Developer Configuration Management | Trusted Generation	Require the developer of the system, system component, or system service to employ tools for comparing newly generated versions of security-relevant hardware descriptions, source code, and object code with previous versions.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SA-10(05)	Developer Configuration Management | Mapping Integrity for Version Control	Require the developer of the system, system component, or system service to maintain the integrity of the mapping between the master build data describing the current version of security-relevant hardware, software, and firmware and the on-site master copy of the data for the current version.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SA-10(06)	Developer Configuration Management | Trusted Distribution	Require the developer of the system, system component, or system service to execute procedures for ensuring that security-relevant hardware, software, and firmware updates distributed to the organization are exactly as specified by the master copies.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SA-10(07)	Developer Configuration Management | Security and Privacy Representatives	Require [Assignment: organization-defined security and privacy representatives] to be included in the [Assignment: organization-defined configuration change management and control process].	Functional	Equal	Security, Compliance & Resilience Representatives For Product Changes	TDA-02.7	Mechanisms exist to include appropriate security, compliance and resilience representatives in the product feature and/or functionality change control review process.	10		Not Selected
SA-11	Developer Testing and Evaluation	Require the developer of the system, system component, or system service, at all post-design stages of the system development life cycle, to:a. Develop and implement a plan for ongoing security and privacy control assessments;b. Perform [Selection (one or more): unit; integration; system; regression] testing/evaluation [Assignment: organization-defined frequency] at [Assignment: organization-defined depth and coverage];c. Produce evidence of the execution of the assessment plan and the results of the testing and evaluation;d. Implement a verifiable flaw remediation process; ande. Correct flaws identified during testing and evaluation.	Functional	Equal	Security, Compliance & Resilience Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and (3) Document the results.	10		Moderate
SA-11(01)	Developer Testing and Evaluation | Static Code Analysis	Require the developer of the system, system component, or system service to employ static code analysis tools to identify common flaws and document the results of the analysis.	Functional	Equal	Static Code Analysis	TDA-09.2	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to employ static code analysis tools to identify and remediate common flaws and document the results of the analysis.	10		Not Selected
SA-11(02)	Developer Testing and Evaluation | Threat Modeling and Vulnerability Analyses	Require the developer of the system, system component, or system service to perform threat modeling and vulnerability analyses during development and the subsequent testing and evaluation of the system, component, or service that:a. Uses the following contextual information: [Assignment: organization-defined information concerning impact, environment of operations, known or assumed threats, and acceptable risk levels];b. Employs the following tools and methods: [Assignment: organization-defined tools and methods];c. Conducts the modeling and analyses at the following level of rigor: [Assignment: organization-defined breadth and depth of modeling and analyses]; andd. Produces evidence that meets the following acceptance criteria: [Assignment: organization-defined acceptance criteria].	Functional	Intersects With	reat Analysis & Flaw	TDA-15	Mechanisms exist to require system developers and integrators to develop and implement an ongoing Security Testing and Evaluation (ST&E) plan, or similar process, to objectively identify and remediate vulnerabilities prior to release to production.	5		Not Selected

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-53B Baseline
SA-11(02)	Developer Testing and Evaluation | Threat Modeling and Vulnerability Analyses	Require the developer of the system, system component, or system service to perform threat modeling and vulnerability analyses during development and the subsequent testing and evaluation of the system, component, or service that:a. Uses the following contextual information: [Assignment: organization-defined information concerning impact, environment of operations, known or assumed threats, and acceptable risk levels];b. Employs the following tools and methods: [Assignment: organization-defined tools and methods];c. Conducts the modeling and analyses at the following level of rigor: [Assignment: organization-defined breadth and depth of modeling and analyses]; andd. Produces evidence that meets the following acceptance criteria: [Assignment: organization-defined acceptance criteria].	Functional	Intersects With	Threat Modeling	TDA-06.2	Mechanisms exist to perform threat modelling and other secure design techniques, to ensure that threats to software and solutions are identified and accounted for.	5		Not Selected
SA-11(03)	Developer Testing and Evaluation | Independent Verification of Assessment Plans and Evidence	a. Require an independent agent satisfying [Assignment: organization-defined independence criteria] to verify the correct implementation of the developer security and privacy assessment plans and the evidence produced during testing and evaluation; andb. Verify that the independent agent is provided with sufficient information to complete the verification process or granted the authority to obtain such information.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SA-11(04)	Developer Testing and Evaluation | Manual Code Reviews	Require the developer of the system, system component, or system service to perform a manual code review of [Assignment: organization-defined specific code] using the following processes, procedures, and/or techniques: [Assignment: organization-defined processes, procedures, and/or techniques].	Functional	Equal	Manual Code Review	TDA-09.7	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to employ a manual code review process to identify and remediate unique flaws that require knowledge of the application's requirements and	10		Not Selected
SA-11(05)	Developer Testing and Evaluation | Penetration Testing	Require the developer of the system, system component, or system service to perform penetration testing:a. At the following level of rigor: [Assignment: organization-defined breadth and depth of testing]; andb. Under the following constraints: [Assignment: organization-defined constraints].	Functional	Intersects With	Threat Analysis & Flaw Remediation During Development	IAO-04	Mechanisms exist to require system developers and integrators to create and execute a Security Testing and Evaluation (ST&E) plan, or similar process, to identify and remediate flaws during development.	5		Not Selected
SA-11(05)	Developer Testing and Evaluation | Penetration Testing	Require the developer of the system, system component, or system service to perform penetration testing:a. At the following level of rigor: [Assignment: organization-defined breadth and depth of testing]; andb. Under the following constraints: [Assignment: organization-defined constraints].	Functional	Intersects With	Application Penetration Testing	TDA-09.5	Mechanisms exist to perform application-level penetration testing of custom-made Technology Assets, Applications and/or Services (TAAS).	5		Not Selected
SA-11(05)	Developer Testing and Evaluation | Penetration Testing	Require the developer of the system, system component, or system service to perform penetration testing:a. At the following level of rigor: [Assignment: organization-defined breadth and depth of testing]; andb. Under the following constraints: [Assignment: organization-defined constraints].	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and (3) Document the results.	5		Not Selected
SA-11(05)	Developer Testing and Evaluation | Penetration Testing	Require the developer of the system, system component, or system service to perform penetration testing:a. At the following level of rigor: [Assignment: organization-defined breadth and depth of testing]; andb. Under the following constraints: [Assignment: organization-defined constraints].	Functional	Intersects With	Specialized Assessments	IAO-02.2	Mechanisms exist to conduct specialized assessments for: (1) Statutory, regulatory and contractual compliance obligations; (2) Monitoring capabilities; (3) Mobile devices; (4) Databases; (5) Application security; (6) Embedded technologies (e.g., IoT, OT, etc.); (7) Vulnerability management; (8) Malicious code; (9) Insider threats; (10) Performance/load testing; and/or (11) Artificial Intelligence and Autonomous Technologies (AAT).	5		Not Selected
SA-11(05)	Developer Testing and Evaluation | Penetration Testing	Require the developer of the system, system component, or system service to perform penetration testing:a. At the following level of rigor: [Assignment: organization-defined breadth and depth of testing]; andb. Under the following constraints: [Assignment: organization-defined constraints].	Functional	Intersects With	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	5		Not Selected
SA-11(06)	Developer Testing and Evaluation | Attack Surface Reviews	Require the developer of the system, system component, or system service to perform attack surface reviews.	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and (3) Document the results.	5		Not Selected
SA-11(06)	Developer Testing and Evaluation | Attack Surface Reviews	Require the developer of the system, system component, or system service to perform attack surface reviews.	Functional	Intersects With	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	5		Not Selected
SA-11(07)	Developer Testing and Evaluation | Verify Scope of Testing and Evaluation	Require the developer of the system, system component, or system service to verify that the scope of testing and evaluation provides complete coverage of the required controls at the following level of rigor: [Assignment: organization-defined breadth and depth of testing and evaluation].	Functional	Intersects With	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	5		Not Selected
SA-11(07)	Developer Testing and Evaluation | Verify Scope of Testing and Evaluation	Require the developer of the system, system component, or system service to verify that the scope of testing and evaluation provides complete coverage of the required controls at the following level of rigor: [Assignment: organization-defined breadth and depth of testing and evaluation].	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and (3) Document the results.	5		Not Selected
SA-11(08)	Developer Testing and Evaluation | Dynamic Code Analysis	Require the developer of the system, system component, or system service to employ dynamic code analysis tools to identify common flaws and document the results of the analysis.	Functional	Equal	Dynamic Code Analysis	TDA-09.3	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to employ dynamic code analysis tools to identify and remediate common flaws and document the results of the analysis.	10		Not Selected
SA-11(09)	Developer Testing and Evaluation | Interactive Application Security Testing	Require the developer of the system, system component, or system service to employ interactive application security testing tools to identify flaws and document the results.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-53B Baseline
SA-12		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SA-12(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SA-12(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SA-12(03)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SA-12(04)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SA-12(05)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SA-12(06)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SA-12(07)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SA-12(08)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SA-12(09)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SA-12(10)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SA-12(11)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SA-12(12)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SA-12(13)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SA-12(14)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SA-12(15)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SA-13		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SA-14		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SA-14(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SA-15	Development Process, Standards, and Tools	a. Require the developer of the system, system component, or system service to follow a documented development process that:1. Explicitly addresses security and privacy requirements;2. Identifies the standards and tools used in the development process;3. Documents the specific tool options and tool configurations used in the development process; and4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; andb. Review the development process, standards, tools, tool options, and tool configurations [Assignment: organization-defined frequency] to determine if the process, standards, tools, tool options and tool configurations selected and employed can satisfy the following security and privacy requirements: [Assignment: organization-defined security and privacy requirements].	Functional	Equal	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	10		Moderate
SA-15(01)	Development Process, Standards, and Tools | Quality Metrics	Require the developer of the system, system component, or system service to:a. Define quality metrics at the beginning of the development process; andb. Provide evidence of meeting the quality metrics [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined program review milestones]; upon delivery].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SA-15(02)	Development Process, Standards, and Tools | Security and Privacy Tracking Tools	Require the developer of the system, system component, or system service to select and employ security and privacy tracking tools for use during the development process.	Functional	Equal	Capabilities Deficiency Tracking	IAO-05	control; (3) Description of the deficiency(ies); (4) Risk associated with the deficiency(ies); (5) Source deficiency identification/detection; (6) Temporary compensating controls, if applicable; (7) Point of Contact (POC) (e.g.	10		Not Selected
SA-15(03)	Development Process, Standards, and Tools | Criticality Analysis	Require the developer of the system, system component, or system service to perform a criticality analysis:a. At the following decision points in the system development life cycle: [Assignment: organization-defined decision points in the system development life cycle]; andb. At the following level of rigor: [Assignment: organization-defined breadth and depth of criticality analysis].	Functional	Equal	Criticality Analysis During Development	TDA-06.1	Mechanisms exist to require the developer of the Technology Asset, Application and/or Service (TAAS) to perform a criticality analysis at organization-defined decision points in the Secure Development Life Cycle (SDLC).	10		Moderate
SA-15(04)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SA-15(05)	Development Process, Standards, and Tools | Attack Surface Reduction	Require the developer of the system, system component, or system service to reduce attack surfaces to [Assignment: organization-defined thresholds].	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening	5		Not Selected
SA-15(05)	Development Process, Standards, and Tools | Attack Surface Reduction	Require the developer of the system, system component, or system service to reduce attack surfaces to [Assignment: organization-defined thresholds].	Functional	Intersects With	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or	5		Not Selected
SA-15(06)	Development Process, Standards, and Tools | Continuous Improvement	Require the developer of the system, system component, or system service to implement an explicit process to continuously improve the development process.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SA-15(07)	Development Process, Standards, and Tools | Automated Vulnerability Analysis	Require the developer of the system, system component, or system service [Assignment: organization-defined frequency] to:a. Perform an automated vulnerability analysis using [Assignment: organization-defined tools];b. Determine the exploitation potential for discovered vulnerabilities;c. Determine potential risk mitigations for delivered vulnerabilities; andd. Deliver the outputs of the tools and results of the analysis to [Assignment: organization-defined personnel or roles].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SA-15(08)	Development Process, Standards, and Tools | Reuse of Threat and Vulnerability Information	Require the developer of the system, system component, or system service to use threat modeling and vulnerability analyses from similar systems, components, or services to inform the current development process.	Functional	Equal	Threat Modeling	TDA-06.2	Mechanisms exist to perform threat modelling and other secure design techniques, to ensure that threats to software and solutions are identified and accounted for.	10		Not Selected
SA-15(09)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SA-15(10)	Development Process, Standards, and Tools | Incident Response Plan	Require the developer of the system, system component, or system service to provide, implement, and test an incident response plan.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SA-15(11)	Development Process, Standards, and Tools | Archive System or Component	Require the developer of the system or system component to archive the system or component to be released or delivered together with the corresponding evidence supporting the final security and privacy review.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SA-15(12)	Development Process, Standards, and Tools | Minimize Personally Identifiable Information	Require the developer of the system or system component to minimize the use of personally identifiable information in development and test environments.	Functional	Equal	Limit Sensitive / Regulated Data In Testing, Training & Research	DCH-18.2	Mechanisms exist to minimize the use of sensitive/regulated data for research, testing, or training, in accordance with authorized, legitimate business practices.	10		Not Selected
SA-15(13)	Development Process, Standards, and Tools | Logging Syntax	Require the developer of the system, system component, or system service to use [Assignment: organization-defined secure logging format] to log [assignment: organization-defined event types] at [assignment: organization-defined level of detail].	Functional	Equal	Logging Syntax	TDA-02.14	Mechanisms exist to require system developers to use an industry-defined secure logging format to generate event logs for specified event types at organization-defined level of	10		Not Selected
SA-16	Developer-provided Training	Require the developer of the system, system component, or system service to provide the following training on the correct use and operation of the implemented security and privacy functions, controls, and/or mechanisms: [Assignment: organization-defined training].	Functional	Equal	Developer-Provided Training	TDA-16	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to provide training on the correct use and operation of the Technology Asset, Application and/or Service (TAAS).	10		High

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-53B Baseline
SA-17	Developer Security and Privacy Architecture and Design	Require the developer of the system, system component, or system service to produce a design specification and security and privacy architecture that:a. Is consistent with the organization's security and privacy architecture that is an integral part the organization's enterprise architecture;b. Accurately and completely describes the required security and privacy functionality, and the allocation of controls among physical and logical components; andc. Expresses how individual security and privacy functions, mechanisms, and services work together to provide required security and privacy capabilities and a unified approach to protection.	Functional	Equal	Developer Architecture & Design	TDA-05	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to produce a design specification and security architecture that: (1) 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; (2) Accurately and completely describes the required security functionality and the allocation of security, compliance and resilience controls among physical and logical components; and (3) Expresses how individual security functions, mechanisms and services work together to	10		High
SA-17(01)	Developer Security and Privacy Architecture and Design | Formal Policy Model	Require the developer of the system, system component, or system service to:a. Produce, as an integral part of the development process, a formal policy model describing the [Assignment: organization-defined elements of organizational security and privacy policy] to be enforced; andb. Prove that the formal policy model is internally consistent and sufficient to enforce the defined elements of the organizational security and privacy policy when implemented.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SA-17(02)	Developer Security and Privacy Architecture and Design | Security-relevant Components	Require the developer of the system, system component, or system service to:a. Define security-relevant hardware, software, and firmware; andb. Provide a rationale that the definition for security-relevant hardware, software, and firmware is	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SA-17(03)	Developer Security and Privacy Architecture and Design | Formal Correspondence	Require the developer of the system, system component, or system service to:a. Produce, as an integral part of the development process, a formal top-level specification that specifies the interfaces to security-relevant hardware, software, and firmware in terms of exceptions, error messages, and effects;b. Show via proof to the extent feasible with additional informal demonstration as necessary, that the formal top-level specification is consistent with the formal policy model;c. Show via informal demonstration, that the formal top-level specification completely covers the interfaces to security-relevant hardware, software, and firmware;d. Show that the formal top-level specification is an accurate description of the implemented security-relevant hardware, software, and firmware; ande. Describe the security-relevant hardware, software, and firmware mechanisms not addressed in the formal top-level specification but strictly internal to the security-relevant hardware, software, and firmware.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SA-17(04)	Developer Security and Privacy Architecture and Design | Informal Correspondence	Require the developer of the system, system component, or system service to:a. Produce, as an integral part of the development process, an informal descriptive top-level specification that specifies the interfaces to security-relevant hardware, software, and firmware in terms of exceptions, error messages, and effects;b. Show via [Selection (one): informal demonstration; convincing argument with formal methods as feasible] that the descriptive top-level specification is consistent with the formal policy model;c. Show via informal demonstration, that the descriptive top-level specification completely covers the interfaces to security-relevant hardware, software, and firmware;d. Show that the descriptive top-level specification is an accurate description of the interfaces to security-relevant hardware, software, and firmware; ande. Describe the security-relevant hardware, software, and firmware mechanisms not addressed in the descriptive top-level specification but strictly internal to the security-relevant hardware, software, and firmware.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SA-17(05)	Developer Security and Privacy Architecture and Design | Conceptually Simple Design	Require the developer of the system, system component, or system service to:a. Design and structure the security-relevant hardware, software, and firmware to use a complete, conceptually simple protection mechanism with precisely defined semantics; andb. Internally structure the security-relevant hardware, software, and firmware with specific regard for this mechanism.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SA-17(06)	Developer Security and Privacy Architecture and Design | Structure for Testing	Require the developer of the system, system component, or system service to structure security-relevant hardware, software, and firmware to facilitate testing.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SA-17(07)	Developer Security and Privacy Architecture and Design | Structure for Least Privilege	Require the developer of the system, system component, or system service to structure security-relevant hardware, software, and firmware to facilitate controlling access with least privilege.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SA-17(08)	Developer Security and Privacy Architecture and Design | Orchestration	Design [Assignment: organization-defined critical systems or system components] with coordinated behavior to implement the following capabilities: [Assignment: organization-defined capabilities, by system or component].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SA-17(09)	Developer Security and Privacy Architecture and Design | Design Diversity	Use different designs for [Assignment: organization-defined critical systems or system components] to satisfy a common set of requirements or to provide equivalent functionality.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SA-18		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SA-18(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SA-18(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SA-19		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SA-19(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SA-19(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SA-19(03)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SA-19(04)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SA-20	Customized Development of Critical Components	Reimplement or custom develop the following critical system components: [Assignment: organization-defined critical system components].	Functional	Equal	Customized Development of Critical Components	TDA-12	Mechanisms exist to custom-develop critical system components, when Commercial Off The Shelf (COTS) solutions are unavailable.	10		Not Selected
SA-21	Developer Screening	Require that the developer of [Assignment: organization-defined system, system component, or system service]:a. Has appropriate access authorizations as determined by assigned [Assignment: organization-defined official government duties]; andb. Satisfies the following additional personnel screening criteria: [Assignment: organization-defined additional personnel screening criteria].	Functional	Equal	Developer Screening	TDA-13	Mechanisms exist to ensure that the developers of Technology Assets, Applications and/or Services (TAAS) have the requisite skillset and appropriate access authorizations.	10		High
SA-21(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-53B Baseline
SA-22	Unsupported System Components	a. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; orb. Provide the following options for alternative sources for continued support for unsupported components [Selection (one or more): in-house support; [Assignment: organization-defined support from external providers]].	Functional	Intersects With	Unsupported Technology Assets, Applications and/or Services (TAAS)	TDA-17	Mechanisms exist to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by: (1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and (2) Requiring justification and documented approval for the continued use of unsupported TAAS required to satisfy	5		Low
SA-22	Unsupported System Components	a. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; orb. Provide the following options for alternative sources for continued support for unsupported components [Selection (one or more): in-house support; [Assignment: organization-defined support from external providers]].	Functional	Intersects With	Alternate Sources for Continued Support	TDA-17.1	Mechanisms exist to provide in-house support or contract external providers for support with unsupported Technology Assets, Applications and/or Services (TAAS).	5		Low
SA-22(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SA-23	Specialization	Employ [Selection (one or more): design; modification; augmentation; reconfiguration] on [Assignment: organization-defined systems or system components] supporting mission essential services or functions to increase the trustworthiness in those systems or components.	Functional	Intersects With	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	5		Not Selected
SA-23	Specialization	Employ [Selection (one or more): design; modification; augmentation; reconfiguration] on [Assignment: organization-defined systems or system components] supporting mission essential services or functions to increase the trustworthiness in those systems or components.	Functional	Intersects With	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or	5		Not Selected
SA-23	Specialization	Employ [Selection (one or more): design; modification; augmentation; reconfiguration] on [Assignment: organization-defined systems or system components] supporting mission essential services or functions to increase the trustworthiness in those systems or components.	Functional	Intersects With	Customized Development of Critical Components	TDA-12	Mechanisms exist to custom-develop critical system components, when Commercial Off The Shelf (COTS) solutions are unavailable.	5		Not Selected
SC-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and communications protection policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and communications protection policy and procedures; andc. Review and update the current system and communications protection:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5		Low
SC-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and communications protection policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and communications protection policy and procedures; andc. Review and update the current system and communications protection:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Subset Of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10		Low
SC-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and communications protection policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and communications protection policy and procedures; andc. Review and update the current system and communications protection:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	10		Low
SC-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and communications protection policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and communications protection policy and procedures; andc. Review and update the current system and communications protection:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5		Low

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-53B Baseline
SC-02	Separation of System and User Functionality	Separate user functionality, including user interface services, from system management functionality.	Functional	Equal	Application Partitioning	SEA-03.2	Mechanisms exist to separate user functionality from system management functionality.	10		Moderate
SC-02(01)	Separation of System and User Functionality | Interfaces for Non-privileged Users	Prevent the presentation of system management functionality at interfaces to non-privileged users.	Functional	Equal	Application Partitioning	SEA-03.2	Mechanisms exist to separate user functionality from system management functionality.	10		Not Selected
SC-02(02)	Separation of System and User Functionality | Disassociability	Store state information from applications and software separately.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SC-03	Security Function Isolation	Isolate security functions from nonsecurity functions.	Functional	Intersects With	Restrict Access To Security Functions	END-16	Mechanisms exist to ensure security functions are restricted to authorized individuals and enforce least privilege control requirements for necessary job functions.	5		High
SC-03	Security Function Isolation	Isolate security functions from nonsecurity functions.	Functional	Intersects With	Security Function Isolation	SEA-04.1	Mechanisms exist to isolate security functions from non-security functions.	5		High
SC-03(01)	Security Function Isolation | Hardware Separation	Employ hardware separation mechanisms to implement security function isolation.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SC-03(02)	Security Function Isolation | Access and Flow Control Functions	Isolate security functions enforcing access and information flow control from nonsecurity functions and from other security functions.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SC-03(03)	Security Function Isolation | Minimize Nonsecurity Functionality	Minimize the number of nonsecurity functions included within the isolation boundary containing security functions.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SC-03(04)	Security Function Isolation | Module Coupling and Cohesiveness	Implement security functions as largely independent modules that maximize internal cohesiveness within modules and minimize coupling between modules.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SC-03(05)	Security Function Isolation | Layered Structures	Implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.	Functional	Equal	Defense-In-Depth (DiD) Architecture	SEA-03	Mechanisms exist to implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.	10		Not Selected
SC-04	Information in Shared System Resources	Prevent unauthorized and unintended information transfer via shared system resources.	Functional	Equal	Information In Shared Resources	SEA-05	Mechanisms exist to prevent unauthorized and unintended information transfer via shared system resources.	10		Moderate
SC-04(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SC-04(02)	Information in Shared System Resources | Multilevel or Periods Processing	Prevent unauthorized information transfer via shared resources in accordance with [Assignment: organization-defined procedures] when system processing explicitly switches between different information classification levels or security categories.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SC-05	Denial-of-service Protection	a. [Selection (one): Protect against; Limit] the effects of the following types of denial-of-service events: [Assignment: organization-defined types of denial-of-service events]; andb. Employ the following controls to achieve the denial-of-service objective: [Assignment: organization-defined controls by type of denial-of-service event].	Functional	Intersects With	Resource Priority	CAP-02	Mechanisms exist to control resource utilization of Technology Assets, Applications and/or Services (TAAS) that are susceptible to Denial of Service (DoS) attacks to limit and prioritize the use of resources.	5		Low
SC-05	Denial-of-service Protection	a. [Selection (one): Protect against; Limit] the effects of the following types of denial-of-service events: [Assignment: organization-defined types of denial-of-service events]; andb. Employ the following controls to achieve the denial-of-service objective: [Assignment: organization-defined controls by type of denial-of-service event].	Functional	Intersects With	Capacity Planning	CAP-03	Mechanisms exist to conduct capacity planning so that necessary capacity for information processing, telecommunications and environmental support will exist during contingency operations.	5		Low
SC-05	Denial-of-service Protection	a. [Selection (one): Protect against; Limit] the effects of the following types of denial-of-service events: [Assignment: organization-defined types of denial-of-service events]; andb. Employ the following controls to achieve the denial-of-service objective: [Assignment: organization-defined controls by type of denial-of-service event].	Functional	Intersects With	Capacity & Performance Management	CAP-01	Mechanisms exist to facilitate the implementation of capacity management controls to ensure optimal system performance to meet expected and anticipated future capacity requirements.	5		Low
SC-05	Denial-of-service Protection	a. [Selection (one): Protect against; Limit] the effects of the following types of denial-of-service events: [Assignment: organization-defined types of denial-of-service events]; andb. Employ the following controls to achieve the denial-of-service objective: [Assignment: organization-defined controls by type of denial-of-service event].	Functional	Intersects With	Denial of Service (DoS) Protection	NET-02.1	Automated mechanisms exist to protect against or limit the effects of denial of service attacks.	5		Low
SC-05(01)	Denial-of-service Protection | Restrict Ability to Attack Other Systems	Restrict the ability of individuals to launch the following denial-of-service attacks against other systems: [Assignment: organization-defined denial-of-service attacks].	Functional	Intersects With	Resource Priority	CAP-02	Mechanisms exist to control resource utilization of Technology Assets, Applications and/or Services (TAAS) that are susceptible to Denial of Service (DoS) attacks to limit and prioritize the use of resources.	5		Not Selected
SC-05(02)	Denial-of-service Protection | Capacity, Bandwidth, and Redundancy	Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding denial-of-service attacks.	Functional	Intersects With	Resource Priority	CAP-02	Mechanisms exist to control resource utilization of Technology Assets, Applications and/or Services (TAAS) that are susceptible to Denial of Service (DoS) attacks to limit and prioritize the use of resources.	5		Not Selected
SC-05(02)	Denial-of-service Protection | Capacity, Bandwidth, and Redundancy	Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding denial-of-service attacks.	Functional	Intersects With	Capacity Planning	CAP-03	Mechanisms exist to conduct capacity planning so that necessary capacity for information processing, telecommunications and environmental support will exist during contingency operations.	5		Not Selected
SC-05(03)	Denial-of-service Protection | Detection and Monitoring	a. Employ the following monitoring tools to detect indicators of denial-of-service attacks against, or launched from, the system: [Assignment: organization-defined monitoring tools]; andb. Monitor the following system resources to determine if sufficient resources exist to prevent effective denial-of-service attacks: [Assignment: organization-defined system resources].	Functional	Intersects With	Capacity & Performance Management	CAP-01	Mechanisms exist to facilitate the implementation of capacity management controls to ensure optimal system performance to meet expected and anticipated future capacity requirements.	5		Not Selected
SC-06	Resource Availability	Protect the availability of resources by allocating [Assignment: organization-defined resources] by [Selection (one or more): priority; quota; [Assignment: organization-defined controls]].	Functional	Intersects With	Resource Priority	CAP-02	Mechanisms exist to control resource utilization of Technology Assets, Applications and/or Services (TAAS) that are susceptible to Denial of Service (DoS) attacks to limit and prioritize the use of resources.	5		Not Selected
SC-07	Boundary Protection	a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system;b. Implement subnetworks for publicly accessible system components that are [Selection (one): physically; logically] separated from internal organizational networks; andc. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.	Functional	Intersects With	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	5		Low
SC-07(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SC-07(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SC-07(03)	Boundary Protection | Access Points	Limit the number of external network connections to the system.	Functional	Equal	Limit Network Connections	NET-03.1	Mechanisms exist to limit the number of concurrent external network connections to its Technology Assets, Applications and/or Services (TAAS).	10		Moderate

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-53B Baseline
SC-07(04)	Boundary Protection | External Telecommunications Services	a. Implement a managed interface for each external telecommunication service;b. Establish a traffic flow policy for each managed interface;c. Protect the confidentiality and integrity of the information being transmitted across each interface;d. Document each exception to the traffic flow policy with a supporting mission or business need and duration of that need;e. Review exceptions to the traffic flow policy [Assignment: organization-defined frequency] and remove exceptions that are no longer supported by an explicit mission or business need;f. Prevent unauthorized exchange of control plane traffic with external networks;g. Publish information to enable remote networks to detect unauthorized control plane traffic from internal networks; andh. Filter unauthorized control plane traffic from external networks.	Functional	Intersects With	External Telecommunications Services	NET-03.2	Mechanisms exist to maintain a managed interface for each external telecommunication service that protects the confidentiality and integrity of the information being transmitted across each interface.	5		Moderate
SC-07(05)	Boundary Protection | Deny by Default — Allow by Exception	Deny network communications traffic by default and allow network communications traffic by exception (Selection (one or more): at managed interfaces; for [Assignment: organization-defined systems]].	Functional	Intersects With	Deny Traffic by Default & Allow Traffic by Exception	NET-04.1	Mechanisms exist to configure firewall and router configurations to deny network traffic by default and allow network traffic by exception (e.g., deny all, permit by exception).	5		Moderate
SC-07(06)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SC-07(07)	Boundary Protection | Split Tunneling for Remote Devices	Prevent split tunneling for remote devices connecting to organizational systems unless the split tunnel is securely provisioned using [Assignment: organization-defined safeguards].	Functional	Equal	Split Tunneling	CFG-03.4	Mechanisms exist to prevent split tunneling for remote devices unless the split tunnel is securely provisioned using organization-defined safeguards.	10		Moderate
SC-07(08)	Boundary Protection | Route Traffic to Authenticated Proxy Servers	Route [Assignment: organization-defined internal communications traffic] to [Assignment: organization-defined external networks] through authenticated proxy servers at managed interfaces.	Functional	Intersects With	Route Internal Traffic to Proxy Servers	NET-18.1	Mechanisms exist to route internal communications traffic to external networks through organization-approved proxy servers at managed interfaces.	5		Moderate
SC-07(08)	Boundary Protection | Route Traffic to Authenticated Proxy Servers	Route [Assignment: organization-defined internal communications traffic] to [Assignment: organization-defined external networks] through authenticated proxy servers at managed interfaces.	Functional	Intersects With	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	5		Moderate
SC-07(09)	Boundary Protection | Restrict Threatening Outgoing Communications Traffic	a. Detect and deny outgoing communications traffic posing a threat to external systems; andb. Audit the identity of internal users associated with denied communications.	Functional	Intersects With	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	5		Not Selected
SC-07(09)	Boundary Protection | Restrict Threatening Outgoing Communications Traffic	a. Detect and deny outgoing communications traffic posing a threat to external systems; andb. Audit the identity of internal users associated with denied communications.	Functional	Intersects With	External Telecommunications Services	NET-03.2	Mechanisms exist to maintain a managed interface for each external telecommunication service that protects the confidentiality and integrity of the information being transmitted across each interface.	5		Not Selected
SC-07(10)	Boundary Protection | Prevent Exfiltration	a. Prevent the exfiltration of information; andb. Conduct exfiltration tests [Assignment: organization-defined frequency].	Functional	Intersects With	Prevent Unauthorized Exfiltration	NET-03.5	Automated mechanisms exist to prevent the unauthorized exfiltration of sensitive/regulated data across managed interfaces.	5		Not Selected
SC-07(10)	Boundary Protection | Prevent Exfiltration	a. Prevent the exfiltration of information; andb. Conduct exfiltration tests [Assignment: organization-defined frequency].	Functional	Intersects With	Data Loss Prevention (DLP)	NET-17	Automated mechanisms exist to implement Data Loss Prevention (DLP) to protect sensitive information as it is stored, transmitted and processed.	5		Not Selected
SC-07(11)	Boundary Protection | Restrict Incoming Communications Traffic	Only allow incoming communications from [Assignment: organization-defined authorized sources] to be routed to [Assignment: organization-defined authorized destinations].	Functional	Intersects With	Deny Traffic by Default & Allow Traffic by Exception	NET-04.1	Mechanisms exist to configure firewall and router configurations to deny network traffic by default and allow network traffic by exception (e.g., deny all, permit by exception).	5		Not Selected
SC-07(11)	Boundary Protection | Restrict Incoming Communications Traffic	Only allow incoming communications from [Assignment: organization-defined authorized sources] to be routed to [Assignment: organization-defined authorized destinations].	Functional	Intersects With	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	5		Not Selected
SC-07(12)	Boundary Protection | Host-based Protection	Implement [Assignment: organization-defined host-based boundary protection mechanisms] at [Assignment: organization-defined system components].	Functional	Equal	Host-Based Security Function Isolation	END-16.1	Mechanisms exist to implement underlying software separation mechanisms to facilitate security function isolation.	10		Not Selected
SC-07(13)	Boundary Protection | Isolation of Security Tools, Mechanisms, and Support Components	Isolate [Assignment: organization-defined information security tools, mechanisms, and support components] from other internal system components by implementing physically separate subnetworks with managed interfaces to other components of the system.	Functional	Intersects With	Security Management Subnets	NET-06.1	Mechanisms exist to implement security management subnets to isolate security tools and support components from other internal system components by implementing separate subnetworks with managed interfaces to other components of the system.	5		Not Selected
SC-07(14)	Boundary Protection | Protect Against Unauthorized Physical Connections	Protect against unauthorized physical connections at [Assignment: organization-defined managed interfaces].	Functional	Intersects With	Equipment Siting & Protection	PES-12	Physical security mechanisms exist to locate system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.	5		Not Selected
SC-07(14)	Boundary Protection | Protect Against Unauthorized Physical Connections	Protect against unauthorized physical connections at [Assignment: organization-defined managed interfaces].	Functional	Intersects With	Lockable Physical Casings	PES-03.2	Physical access control mechanisms exist to protect system components from unauthorized physical access (e.g., lockable physical casings).	5		Not Selected
SC-07(14)	Boundary Protection | Protect Against Unauthorized Physical Connections	Protect against unauthorized physical connections at [Assignment: organization-defined managed interfaces].	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5		Not Selected
SC-07(15)	Boundary Protection | Networked Privileged Accesses	Route networked, privileged accesses through a dedicated, managed interface for purposes of access control and auditing.	Functional	Equal	Route Privileged Network Access	NET-18.3	Automated mechanisms exist to route networked, privileged accesses through a dedicated, managed interface for purposes of access control and auditing.	10		Not Selected
SC-07(16)	Boundary Protection | Prevent Discovery of System Components	Prevent the discovery of specific system components that represent a managed interface.	Functional	Equal	Prevent Discovery of Internal Information	NET-03.3	Mechanisms exist to prevent the public disclosure of internal network information.	10		Not Selected
SC-07(17)	Boundary Protection | Automated Enforcement of Protocol Formats	Enforce adherence to protocol formats.	Functional	Equal	Web Application Firewall (WAF)	WEB-03	Mechanisms exist to deploy Web Application Firewalls (WAFs) to provide defense-in-depth protection for application-specific threats.	10		Not Selected
SC-07(18)	Boundary Protection | Fail Secure	Prevent systems from entering unsecure states in the event of an operational failure of a boundary protection device.	Functional	Intersects With	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or	5		High
SC-07(19)	Boundary Protection | Block Communication from Non-organizationally Configured Hosts	Block inbound and outbound communications traffic between [Assignment: organization-defined communication clients] that are independently configured by end users and external service providers.	Functional	Intersects With	Network Access Control (NAC)	AST-02.5	Automated mechanisms exist to employ Network Access Control (NAC), or a similar technology, which is capable of detecting unauthorized devices and disable network access to those unauthorized devices.	5		Not Selected
SC-07(20)	Boundary Protection | Dynamic Isolation and Segregation	Provide the capability to dynamically isolate [Assignment: organization-defined system components] from other system components.	Functional	Equal	Dynamic Isolation & Segregation (Sandboxing)	NET-03.6	Automated mechanisms exist to dynamically isolate (e.g., sandbox) untrusted components during runtime, where the component is isolated in a fault-contained environment but it can still collaborate with the application.	10		Not Selected

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-53B Baseline
SC-07(21)	Boundary Protection | Isolation of System Components	Employ boundary protection mechanisms to isolate [Assignment: organization-defined system components] supporting [Assignment: organization-defined missions and/or business functions].	Functional	Equal	Isolation of System Components	NET-03.7	Mechanisms exist to employ boundary protections to isolate Technology Assets, Applications and/or Services (TAAS) that support critical missions and/or business functions.	10		High
SC-07(22)	Boundary Protection | Separate Subnets for Connecting to Different Security Domains	Implement separate network addresses to connect to systems in different security domains.	Functional	Intersects With	Separate Subnet for Connecting to Different Security Domains	NET-03.8	Mechanisms exist to implement separate network addresses (e.g., different subnets) to connect to systems in different security domains.	5		Not Selected
SC-07(23)	Boundary Protection | Disable Sender Feedback on Protocol Validation Failure	Disable feedback to senders on protocol format validation failure.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SC-07(24)	Boundary Protection | Personally Identifiable Information	For systems that process personally identifiable information:a. Apply the following processing rules to data elements of personally identifiable information: [Assignment: organization-defined processing rules];b. Monitor for permitted processing at the external interfaces to the system and at key internal boundaries within the system;c. Document each processing exception; andd. Review and remove exceptions that are no longer supported.	Functional	Equal	Personal Data (PD)	NET-03.4	Mechanisms exist to apply network-based processing rules to data elements of Personal Data (PD).	10		Not Selected
SC-07(25)	Boundary Protection | Unclassified National Security System Connections	Prohibit the direct connection of [Assignment: organization-defined unclassified national security system] to an external network without the use of [Assignment: organization-defined boundary protection device].	Functional	Intersects With	Interconnection Security Agreements (ISAs)	NET-05	Mechanisms exist to authorize connections from systems to other systems using Interconnection Security Agreements (ISAs), or similar methods, that document, for each interconnection: (1) Interface characteristics; (2) Security, compliance and resilience requirements; and; (3) The nature of the information	5		Not Selected
SC-07(26)	Boundary Protection | Classified National Security System Connections	Prohibit the direct connection of a classified national security system to an external network without the use of [Assignment: organization-defined boundary protection device].	Functional	Intersects With	Interconnection Security Agreements (ISAs)	NET-05	Mechanisms exist to authorize connections from systems to other systems using Interconnection Security Agreements (ISAs), or similar methods, that document, for each interconnection: (1) Interface characteristics; (2) Security, compliance and resilience requirements; and; (3) The nature of the information	5		Not Selected
SC-07(27)	Boundary Protection | Unclassified Non-national Security System Connections	Prohibit the direct connection of [Assignment: organization-defined unclassified non-national security system] to an external network without the use of [Assignment: organization-defined boundary protection device].	Functional	Equal	External System Connections	NET-05.1	Mechanisms exist to prohibit the direct connection of a sensitive system to an external network without the use of an organization-defined boundary protection device.	10		Not Selected
SC-07(28)	Boundary Protection | Connections to Public Networks	Prohibit the direct connection of [Assignment: organization-defined system] to a public network.	Functional	Equal	Direct Internet Access Restrictions	NET-06.5	Mechanisms exist to prohibit, or strictly-control, Internet access from sensitive/regulated data enclaves (secure zones).	10		Not Selected
SC-07(29)	Boundary Protection | Separate Subnets to Isolate Functions	Implement [Selection (one): physically; logically] separate subnetworks to isolate the following critical system components and functions: [Assignment: organization-defined critical system components and functions].	Functional	Intersects With	Cloud Infrastructure Security Subnet	CLD-03	Mechanisms exist to host security-specific technologies in a dedicated subnet.	5		Not Selected
SC-07(29)	Boundary Protection | Separate Subnets to Isolate Functions	Implement [Selection (one): physically; logically] separate subnetworks to isolate the following critical system components and functions: [Assignment: organization-defined critical system components and functions].	Functional	Intersects With	Security Management Subnets	NET-06.1	Mechanisms exist to implement security management subnets to isolate security tools and support components from other internal system components by implementing separate subnetworks with managed interfaces to other components of the system.	5		Not Selected
SC-07(29)	Boundary Protection | Separate Subnets to Isolate Functions	Implement [Selection (one): physically; logically] separate subnetworks to isolate the following critical system components and functions: [Assignment: organization-defined critical system components and functions].	Functional	Intersects With	Separate Subnet for Connecting to Different Security Domains	NET-03.8	Mechanisms exist to implement separate network addresses (e.g., different subnets) to connect to systems in different security domains.	5		Not Selected
SC-08	Transmission Confidentiality and Integrity	Protect the [Selection (one or more): confidentiality; integrity] of transmitted information.	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5		Moderate
SC-08	Transmission Confidentiality and Integrity	Protect the [Selection (one or more): confidentiality; integrity] of transmitted information.	Functional	Intersects With	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	5		Moderate
SC-08(01)	Transmission Confidentiality and Integrity | Cryptographic Protection	Implement cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.	Functional	Intersects With	Alternate Physical Protection	CRY-01.1	Cryptographic mechanisms exist to prevent unauthorized disclosure of information as an alternative to physical safeguards.	5		Moderate
SC-08(01)	Transmission Confidentiality and Integrity | Cryptographic Protection	Implement cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.	Functional	Intersects With	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	5		Moderate
SC-08(01)	Transmission Confidentiality and Integrity | Cryptographic Protection	Implement cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5		Moderate
SC-08(02)	Transmission Confidentiality and Integrity | Pre- and Post-transmission Handling	Maintain the [Selection (one or more): confidentiality; integrity] of information during preparation for transmission and during reception.	Functional	Intersects With	Pre/Post Transmission Handling	CRY-01.3	Cryptographic mechanisms exist to ensure the confidentiality and integrity of information during preparation for transmission and during reception.	5		Not Selected
SC-08(02)	Transmission Confidentiality and Integrity | Pre- and Post-transmission Handling	Maintain the [Selection (one or more): confidentiality; integrity] of information during preparation for transmission and during reception.	Functional	Intersects With	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	5		Not Selected
SC-08(02)	Transmission Confidentiality and Integrity | Pre- and Post-transmission Handling	Maintain the [Selection (one or more): confidentiality; integrity] of information during preparation for transmission and during reception.	Functional	Intersects With	Media Use	DCH-10	Mechanisms exist to restrict the use of types of digital media on systems or system components.	5		Not Selected
SC-08(03)	Transmission Confidentiality and Integrity | Cryptographic Protection for Message Externals	Implement cryptographic mechanisms to protect message externals unless otherwise protected by [Assignment: organization-defined alternative physical controls].	Functional	Equal	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	10		Not Selected
SC-08(04)	Transmission Confidentiality and Integrity | Conceal or Randomize Communications	Implement cryptographic mechanisms to conceal or randomize communication patterns unless otherwise protected by [Assignment: organization-defined alternative physical controls].	Functional	Equal	Conceal / Randomize Communications	CRY-01.4	Cryptographic mechanisms exist to conceal or randomize communication patterns.	10		Not Selected
SC-08(05)	Transmission Confidentiality and Integrity | Protected Distribution System	Implement [Assignment: organization-defined protected distribution system] to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SC-09		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SC-10	Network Disconnect	Terminate the network connection associated with a communications session at the end of the session or after [Assignment: organization-defined time period] of inactivity.	Functional	Equal	Network Connection Termination	NET-07	Mechanisms exist to terminate network connections at the end of a session or after an organization-defined time period of inactivity.	10		Moderate
SC-11	Trusted Path	a. Provide a [Selection (one): physically; logically] isolated trusted communications path for communications between the user and the trusted components of the system; andb. Permit users to invoke the trusted communications path for communications between the user and the following security functions of the system, including at a minimum, authentication and re-authentication: [Assignment: organization-defined security functions].	Functional	Equal	Trusted Path	END-09	Mechanisms exist to establish a trusted communications path between the user and the security functions of the operating system.	10		Not Selected

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh	Notes	NIST SP 800-53B Baseline
SC-11(01)	Trusted Path | Irrefutable Communications Path	a. Provide a trusted communications path that is irrefutably distinguishable from other communications paths; andb. Initiate the trusted communications path for communications between the [Assignment: organization-defined security functions] of the system and the user.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SC-12	Cryptographic Key Establishment and Management	Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].	Functional	Intersects With	Public Key Infrastructure (PKI)	CRY-08	Mechanisms exist to securely implement an internal Public Key Infrastructure (PKI) infrastructure or obtain PKI services from a reputable PKI service provider.	5		Low
SC-12(01)	Cryptographic Key Establishment and Management | Availability	Maintain availability of information in the event of the loss of cryptographic keys by users.	Functional	Equal	Cryptographic Key Loss or Change	CRY-09.3	Mechanisms exist to ensure the availability of information in the event of the loss of cryptographic keys by individual users.	10		High
SC-12(02)	Cryptographic Key Establishment and Management | Symmetric Keys	Produce, control, and distribute symmetric cryptographic keys using [Selection (one): NIST FIPS-validated; NSA-approved] key management technology and processes.	Functional	Equal	Symmetric Keys	CRY-09.1	Mechanisms exist to facilitate the production and management of symmetric cryptographic keys using Federal Information Processing Standards (FIPS)-compliant key management technology and processes.	10		Not Selected
SC-12(03)	Cryptographic Key Establishment and Management | Asymmetric Keys	Produce, control, and distribute asymmetric cryptographic keys using [Selection (one): NSA-approved key management technology and processes; prepositioned keying material; DoD-approved or DoD-issued Medium Assurance PKI certificates; DoD-approved or DoD-issued Medium Hardware Assurance PKI certificates and hardware security tokens that protect the user's private key; certificates issued in accordance with organization-defined requirements].	Functional	Equal	Asymmetric Keys	CRY-09.2	Mechanisms exist to facilitate the production and management of asymmetric cryptographic keys using Federal Information Processing Standards (FIPS)-compliant key management technology and processes that protect the user's private key.	10		Not Selected
SC-12(04)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SC-12(05)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SC-12(06)	Cryptographic Key Establishment and Management | Physical Control of Keys	Maintain physical control of cryptographic keys when stored information is encrypted by external service providers.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SC-13	Cryptographic Protection	a. Determine the [Assignment: organization-defined cryptographic uses]; andb. Implement the following types of cryptography required for each specified cryptographic use: [Assignment: organization-defined types of cryptography for each specified cryptographic use].	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5		Low
SC-13	Cryptographic Protection	a. Determine the [Assignment: organization-defined cryptographic uses]; andb. Implement the following types of cryptography required for each specified cryptographic use: [Assignment: organization-defined types of cryptography for each specified cryptographic use].	Functional	Intersects With	Export-Controlled Cryptography	CRY-01.2	Mechanisms exist to address the exporting of cryptographic technologies in compliance with relevant statutory and regulatory requirements.	5		Low
SC-13	Cryptographic Protection	a. Determine the [Assignment: organization-defined cryptographic uses]; andb. Implement the following types of cryptography required for each specified cryptographic use: [Assignment: organization-defined types of cryptography for each specified cryptographic use].	Functional	Intersects With	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	5		Low
SC-13(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SC-13(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SC-13(03)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SC-13(04)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SC-14		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SC-15	Collaborative Computing Devices and Applications	a. Prohibit remote activation of collaborative computing devices and applications with the following exceptions: [Assignment: organization-defined exceptions where remote activation is to be allowed]; andb. Provide an explicit indication of use to users physically present at the devices.	Functional	Intersects With	Collaborative Computing Devices	END-14	Mechanisms exist to unplug or prohibit the remote activation of collaborative computing devices with the following exceptions: (1) Networked whiteboards; (2) Video teleconference cameras; and (3) Teleconference microphones.	5		Low
SC-15(01)	Collaborative Computing Devices and Applications | Physical or Logical Disconnect	Provide [Selection (one or more): physical; logical] disconnect of collaborative computing devices in a manner that supports ease of use.	Functional	Intersects With	Collaborative Computing Devices	END-14	Mechanisms exist to unplug or prohibit the remote activation of collaborative computing devices with the following exceptions: (1) Networked whiteboards; (2) Video teleconference cameras; and (3) Teleconference microphones.	5		Not Selected
SC-15(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SC-15(03)	Collaborative Computing Devices and Applications | Disabling and Removal in Secure Work Areas	Disable or remove collaborative computing devices and applications from [Assignment: organization-defined systems or system components] in [Assignment: organization-defined secure work areas].	Functional	Equal	Disabling / Removal In Secure Work Areas	END-14.1	Mechanisms exist to disable or remove collaborative computing devices from critical systems and secure work areas.	10		Not Selected
SC-15(04)	Collaborative Computing Devices and Applications | Explicitly Indicate Current Participants	Provide an explicit indication of current participants in [Assignment: organization-defined online meetings and teleconferences].	Functional	Equal	Explicitly Indicate Current Participants	END-14.2	Automated mechanisms exist to provide an explicit indication of current participants in online meetings and teleconferences.	10		Not Selected
SC-16	Transmission of Security and Privacy Attributes	Associate [Assignment: organization-defined security and privacy attributes] with information exchanged between systems and between system components.	Functional	Intersects With	Transmission of Cybersecurity & Data Protection Attributes	CRY-10	Mechanisms exist to associate Technology Assets, Applications and/or Services (TAAS) security attributes with information exchanged between TAAS.	5		Not Selected
SC-16(01)	Transmission of Security and Privacy Attributes | Integrity Verification	Verify the integrity of transmitted security and privacy attributes.	Functional	Intersects With	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	5		Not Selected
SC-16(01)	Transmission of Security and Privacy Attributes | Integrity Verification	Verify the integrity of transmitted security and privacy attributes.	Functional	Intersects With	Transmission of Cybersecurity & Data Protection Attributes	CRY-10	Mechanisms exist to associate Technology Assets, Applications and/or Services (TAAS) security attributes with information exchanged between TAAS.	5		Not Selected
SC-16(02)	Transmission of Security and Privacy Attributes | Anti-spoofing Mechanisms	Implement anti-spoofing mechanisms to prevent adversaries from falsifying the security attributes indicating the successful application of the security process.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SC-16(03)	Transmission of Security and Privacy Attributes | Cryptographic Binding	Implement [Assignment: organization-defined mechanisms or techniques] to bind security and privacy attributes to transmitted information.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SC-17	Public Key Infrastructure Certificates	a. Issue public key certificates under an [Assignment: organization-defined certificate policy] or obtain public key certificates from an approved service provider; andb. Include only approved trust anchors in trust stores or certificate stores managed by the organization.	Functional	Intersects With	Public Key Infrastructure (PKI)	CRY-08	Mechanisms exist to securely implement an internal Public Key Infrastructure (PKI) infrastructure or obtain PKI services from a reputable PKI service provider.	5		Moderate
SC-18	Mobile Code	a. Define acceptable and unacceptable mobile code and mobile code technologies; andb. Authorize, monitor, and control the use of mobile code within the system.	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	5		Moderate
SC-18(01)	Mobile Code | Identify Unacceptable Code and Take Corrective Actions	Identify [Assignment: organization-defined unacceptable mobile code] and take [Assignment: organization-defined corrective actions].	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5		Not Selected
SC-18(01)	Mobile Code | Identify Unacceptable Code and Take Corrective Actions	Identify [Assignment: organization-defined unacceptable mobile code] and take [Assignment: organization-defined corrective actions].	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	5		Not Selected
SC-18(01)	Mobile Code | Identify Unacceptable Code and Take Corrective Actions	Identify [Assignment: organization-defined unacceptable mobile code] and take [Assignment: organization-defined corrective actions].	Functional	Intersects With	Continuous Vulnerability Remediation Activities	VPM-04	Mechanisms exist to address new threats and vulnerabilities on an ongoing basis and ensure assets are protected against known attacks.	5		Not Selected

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-53B Baseline
SC-18(02)	Mobile Code | Acquisition, Development, and Use	Verify that the acquisition, development, and use of mobile code to be deployed in the system meets [Assignment: organization-defined mobile code requirements].	Functional	Intersects With	Software Licensing Restrictions	AST-02.7	Mechanisms exist to protect Intellectual Property (IP) rights with software licensing restrictions.	5		Not Selected
SC-18(02)	Mobile Code | Acquisition, Development, and Use	Verify that the acquisition, development, and use of mobile code to be deployed in the system meets [Assignment: organization-defined mobile code requirements].	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	5		Not Selected
SC-18(03)	Mobile Code | Prevent Downloading and Execution	Prevent the download and execution of [Assignment: organization-defined unacceptable mobile code].	Functional	Intersects With	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	5		Not Selected
SC-18(03)	Mobile Code | Prevent Downloading and Execution	Prevent the download and execution of [Assignment: organization-defined unacceptable mobile code].	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	5		Not Selected
SC-18(04)	Mobile Code | Prevent Automatic Execution	Prevent the automatic execution of mobile code in [Assignment: organization-defined software applications] and enforce [Assignment: organization-defined actions] prior to executing the code.	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	5		Not Selected
SC-18(04)	Mobile Code | Prevent Automatic Execution	Prevent the automatic execution of mobile code in [Assignment: organization-defined software applications] and enforce [Assignment: organization-defined actions] prior to executing the code.	Functional	Intersects With	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	5		Not Selected
SC-18(05)	Mobile Code | Allow Execution Only in Confined Environments	Allow execution of permitted mobile code only in confined virtual machine environments.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SC-19		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SC-20	Secure Name/address Resolution Service (authoritative Source)	a. Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and b. Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.	Functional	Intersects With	Domain Name Service (DNS) Resolution	NET-10	Mechanisms exist to ensure Domain Name Service (DNS) resolution is designed, implemented and managed to protect the security of name / address resolution.	5		Low
SC-20(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SC-20(02)	Secure Name/address Resolution Service (authoritative Source) | Data Origin and Integrity	Provide data origin and integrity protection artifacts for internal name/address resolution queries.	Functional	Intersects With	Domain Name Service (DNS) Resolution	NET-10	Mechanisms exist to ensure Domain Name Service (DNS) resolution is designed, implemented and managed to protect the security of name / address resolution.	5		Not Selected
SC-21	Secure Name/address Resolution Service (recursive or Caching Resolver)	Request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.	Functional	Equal	Secure Name / Address Resolution Service (Recursive or Caching Resolver)	NET-10.2	Mechanisms exist to perform data origin authentication and data integrity verification on the Domain Name Service (DNS) resolution responses received from authoritative sources when requested by client systems.	10		Low
SC-21(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SC-22	Architecture and Provisioning for Name/address Resolution Service	Ensure the systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal and external role separation.	Functional	Equal	Architecture & Provisioning for Name / Address Resolution Service	NET-10.1	Mechanisms exist to ensure systems that collectively provide Domain Name Service (DNS) resolution service are fault-tolerant and implement internal/external role separation.	10		Low
SC-23	Session Authenticity	Protect the authenticity of communications sessions.	Functional	Equal	Session Integrity	NET-09	Mechanisms exist to protect the authenticity and integrity of communications sessions.	10		Moderate
SC-23(01)	Session Authenticity | Invalidate Session Identifiers at Logout	Invalidate session identifiers upon user logout or other session termination.	Functional	Equal	Invalidate Session Identifiers at Logout	NET-09.1	Automated mechanisms exist to invalidate session identifiers upon user logout or other session termination.	10		Not Selected
SC-23(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SC-23(03)	Session Authenticity | Unique System-generated Session Identifiers	Generate a unique session identifier for each session with [Assignment: organization-defined randomness requirements] and recognize only session identifiers that are system-generated.	Functional	Equal	Unique System-Generated Session Identifiers	NET-09.2	Automated mechanisms exist to generate and recognize unique session identifiers for each session.	10		Not Selected
SC-23(04)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SC-23(05)	Session Authenticity | Allowed Certificate Authorities	Only allow the use of [Assignment: organization-defined certificate authorities] for verification of the establishment of protected sessions.	Functional	Equal	Certificate Authorities	CRY-11	Automated mechanisms exist to enable the use of organization-defined Certificate Authorities (CAs) to facilitate the establishment of protected sessions.	10		Not Selected
SC-24	Fail in Known State	Fail to a [Assignment: organization-defined known system state] for the following failures on the indicated components while preserving [Assignment: organization-defined system state information] in failure: [Assignment: list of organization-defined types of system failures on organization-defined system components].	Functional	Intersects With	Fail Secure	SEA-07.2	Mechanisms exist to enable systems to fail to an organization-defined known-state for types of failures, preserving system state information in failure.	5		High
SC-25	Thin Nodes	Employ minimal functionality and information storage on the following system components: [Assignment: organization-defined system components].	Functional	Equal	Thin Nodes	END-11	Mechanisms exist to configure thin nodes to have minimal functionality and information storage.	10		Not Selected
SC-26	Decoys	Include components within organizational systems specifically designed to be the target of malicious attacks for detecting, deflecting, and analyzing such attacks.	Functional	Equal	Honeypots	SEA-11	Mechanisms exist to utilize honeypots that are specifically designed to be the target of malicious attacks for the purpose of detecting, deflecting and analyzing such attacks.	10		Not Selected
SC-26(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SC-27	Platform-independent Applications	Include within organizational systems the following platform independent applications: [Assignment: organization-defined platform-independent applications].	Functional	Equal	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	10		Not Selected
SC-28	Protection of Information at Rest	Protect the [Selection (one or more): confidentiality; integrity] of the following information at rest: [Assignment: organization-defined information at rest].	Functional	Intersects With	Endpoint Protection Measures	END-02	Mechanisms exist to protect the confidentiality, integrity, availability and safety of endpoint devices.	5		Moderate
SC-28	Protection of Information at Rest	Protect the [Selection (one or more): confidentiality; integrity] of the following information at rest: [Assignment: organization-defined information at rest].	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5		Moderate
SC-28(01)	Protection of Information at Rest | Cryptographic Protection	Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information].	Functional	Intersects With	Cryptographic Protection	BCD-11.4	Cryptographic mechanisms exist to prevent the unauthorized disclosure and/or modification of backup information.	5		Moderate
SC-28(01)	Protection of Information at Rest | Cryptographic Protection	Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information].	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5		Moderate
SC-28(01)	Protection of Information at Rest | Cryptographic Protection	Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information].	Functional	Intersects With	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	5		Moderate
SC-28(01)	Protection of Information at Rest | Cryptographic Protection	Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information].	Functional	Intersects With	Encrypting Data In Storage Media	DCH-07.2	Cryptographic mechanisms exist to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.	5		Moderate
SC-28(02)	Protection of Information at Rest | Offline Storage	Remove the following information from online storage and store offline in a secure location: [Assignment: organization-defined information].	Functional	Intersects With	Offline Storage	CRY-05.2	Mechanisms exist to remove unused data from online storage and archive it off-line in a secure location until it can be disposed of according to data retention requirements.	5		Not Selected

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-53B Baseline
SC-28(02)	Protection of Information at Rest | Offline Storage	Remove the following information from online storage and store offline in a secure location: [Assignment: organization-defined information].	Functional	Intersects With	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5		Not Selected
SC-28(03)	Protection of Information at Rest | Cryptographic Keys	Provide protected storage for cryptographic keys [Selection (one): [Assignment: organization-defined safeguards]; hardware-protected key store].	Functional	Equal	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	10		Not Selected
SC-29	Heterogeneity	Employ a diverse set of information technologies for the following system components in the implementation of the system: [Assignment: organization-defined system components].	Functional	Equal	Heterogeneity	SEA-13	Mechanisms exist to utilize a diverse set of technologies for system components to reduce the impact of technical vulnerabilities from the same Original Equipment Manufacturer (OEM).	10		Not Selected
SC-29(01)	Heterogeneity | Virtualization Techniques	Employ virtualization techniques to support the deployment of a diversity of operating systems and applications that are changed [Assignment: organization-defined frequency].	Functional	Equal	Virtualization Techniques	SEA-13.1	Mechanisms exist to utilize virtualization techniques to support the employment of a diversity of operating systems and applications.	10		Not Selected
SC-30	Concealment and Misdirection	Employ the following concealment and misdirection techniques for [Assignment: organization-defined systems] at [Assignment: organization-defined time periods] to confuse and mislead adversaries: [Assignment: organization-defined concealment and misdirection techniques].	Functional	Intersects With	Concealment & Misdirection	SEA-14	Mechanisms exist to utilize concealment and misdirection techniques for Technology Assets, Applications and/or Services (TAAS) to confuse and mislead adversaries.	5		Not Selected
SC-30(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SC-30(02)	Concealment and Misdirection | Randomness	Employ [Assignment: organization-defined techniques] to introduce randomness into organizational operations and assets.	Functional	Equal	Randomness	SEA-14.1	Automated mechanisms exist to introduce randomness into organizational operations and assets.	10		Not Selected
SC-30(03)	Concealment and Misdirection | Change Processing and Storage Locations	Change the location of [Assignment: organization-defined processing and/or storage] [Selection (one): [Assignment: organization-defined time frequency]; at random time intervals].	Functional	Equal	Change Processing & Storage Locations	SEA-14.2	Automated mechanisms exist to change the location of processing and/or storage at random time intervals.	10		Not Selected
SC-30(04)	Concealment and Misdirection | Misleading Information	Employ realistic, but misleading information in [Assignment: organization-defined system components] about its security state or posture.	Functional	Intersects With	Concealment & Misdirection	SEA-14	Mechanisms exist to utilize concealment and misdirection techniques for Technology Assets, Applications and/or Services (TAAS) to confuse and mislead adversaries.	5		Not Selected
SC-30(05)	Concealment and Misdirection | Concealment of System Components	Employ the following techniques to hide or conceal [Assignment: organization-defined system components]: [Assignment: organization-defined techniques].	Functional	Intersects With	Concealment & Misdirection	SEA-14	Mechanisms exist to utilize concealment and misdirection techniques for Technology Assets, Applications and/or Services (TAAS) to confuse and mislead adversaries.	5		Not Selected
SC-31	Covert Channel Analysis	a. Perform a covert channel analysis to identify those aspects of communications within the system that are potential avenues for covert [Selection (one or more): storage; timing] channels; andb. Estimate the maximum bandwidth of those channels.	Functional	Equal	Covert Channel Analysis	MON-15	Mechanisms exist to conduct covert channel analysis to identify aspects of communications that are potential avenues for covert channels.	10		Not Selected
SC-31(01)	Covert Channel Analysis | Test Covert Channels for Exploitability	Test a subset of the identified covert channels to determine the channels that are exploitable.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SC-31(02)	Covert Channel Analysis | Maximum Bandwidth	Reduce the maximum bandwidth for identified covert [Selection (one or more): storage; timing] channels to [Assignment: organization-defined values].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SC-31(03)	Covert Channel Analysis | Measure Bandwidth in Operational Environments	Measure the bandwidth of [Assignment: organization-defined subset of identified covert channels] in the operational environment of the system.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SC-32	System Partitioning	Partition the system into [Assignment: organization-defined system components] residing in separate [Selection (one): physical; logical] domains or environments based on [Assignment: organization-defined circumstances for physical or logical separation of components].	Functional	Equal	System Partitioning	SEA-03.1	Mechanisms exist to partition systems so that partitions reside in separate physical domains or environments.	10		Not Selected
SC-32(01)	System Partitioning | Separate Physical Domains for Privileged Functions	Partition privileged functions into separate physical domains.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SC-33		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SC-34	Non-modifiable Executable Programs	For [Assignment: organization-defined system components], load and execute:a. The operating environment from hardware-enforced, read-only media; andb. The following applications from hardware-enforced, read-only media: [Assignment: organization-defined applications].	Functional	Equal	Non-Modifiable Executable Programs	SEA-16	Mechanisms exist to utilize non-modifiable executable programs that load and execute the operating environment and applications from hardware-enforced, read-only media.	10		Not Selected
SC-34(01)	Non-modifiable Executable Programs | No Writable Storage	Employ [Assignment: organization-defined system components] with no writeable storage that is persistent across component restart or power on/off.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SC-34(02)	Non-modifiable Executable Programs | Integrity Protection on Read-only Media	Protect the integrity of information prior to storage on read-only media and control the media after such information has been recorded onto the media.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SC-34(03)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SC-35	External Malicious Code Identification	Include system components that proactively seek to identify network-based malicious code or malicious websites.	Functional	Equal	Honeyclients	SEA-12	Mechanisms exist to utilize honeyclients that proactively seek to identify malicious websites and/or web-based malicious code.	10		Not Selected
SC-36	Distributed Processing and Storage	Distribute the following processing and storage components across multiple [Selection (one): physical locations; logical domains]: [Assignment: organization-defined processing and storage components].	Functional	Equal	Distributed Processing & Storage	SEA-15	Mechanisms exist to distribute processing and storage across multiple physical locations.	10		Not Selected
SC-36(01)	Distributed Processing and Storage | Polling Techniques	a. Employ polling techniques to identify potential faults, errors, or compromises to the following processing and storage components: [Assignment: organization-defined distributed processing and storage components]; andb. Take the following actions in response to identified faults, errors, or compromises: [Assignment: organization-defined actions].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SC-36(02)	Distributed Processing and Storage | Synchronization	Synchronize the following duplicate systems or system components: [Assignment: organization-defined duplicate systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SC-37	Out-of-band Channels	Employ the following out-of-band channels for the physical delivery or electronic transmission of [Assignment: organization-defined information, system components, or devices] to [Assignment: organization-defined individuals or systems]: [Assignment: organization-defined out-of-band channels].	Functional	Intersects With	Out-of-Band Channels	NET-11	Mechanisms exist to utilize out-of-band channels for the electronic transmission of information and/or the physical shipment of system components or devices to authorized individuals.	5		Not Selected
SC-37(01)	Out-of-band Channels | Ensure Delivery and Transmission	Employ [Assignment: organization-defined controls] to ensure that only [Assignment: organization-defined individuals or systems] receive the following information, system components, or devices: [Assignment: organization-defined information, system components, or devices].	Functional	Intersects With	Out-of-Band Channels	NET-11	Mechanisms exist to utilize out-of-band channels for the electronic transmission of information and/or the physical shipment of system components or devices to authorized individuals.	5		Not Selected
SC-38	Operations Security	Employ the following operations security controls to protect key organizational information throughout the system development life cycle: [Assignment: organization-defined operations security controls].	Functional	Intersects With	Security Operations Center (SOC)	OPS-04	Mechanisms exist to establish and maintain a Security Operations Center (SOC) that facilitates a 24x7 response capability.	5		Not Selected
SC-38	Operations Security	Employ the following operations security controls to protect key organizational information throughout the system development life cycle: [Assignment: organization-defined operations security controls].	Functional	Intersects With	Operations Security	OPS-01	Mechanisms exist to facilitate the implementation of operational security controls.	5		Not Selected
SC-39	Process Isolation	Maintain a separate execution domain for each executing system process.	Functional	Equal	Process Isolation	SEA-04	Mechanisms exist to implement a separate execution domain for each executing process.	10		Low

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh	Notes	NIST SP 800-53B Baseline
SC-39(01)	Process Isolation | Hardware Separation	Implement hardware separation mechanisms to facilitate process isolation.	Functional	Equal	Hardware Separation	SEA-04.2	Mechanisms exist to implement underlying hardware separation mechanisms to facilitate process separation.	10		Not Selected
SC-39(02)	Process Isolation | Separate Execution Domain Per Thread	Maintain a separate execution domain for each thread in [Assignment: organization-defined multi-threaded processing].	Functional	Equal	Thread Separation	SEA-04.3	Mechanisms exist to maintain a separate execution domain for each thread in multi-threaded processing.	10		Not Selected
SC-40	Wireless Link Protection	Protect external and internal [Assignment: organization-defined wireless links] from the following signal parameter attacks: [Assignment: organization-defined types of signal parameter attacks or references to sources for such attacks].	Functional	Intersects With	Wireless Link Protection	NET-12.1	Mechanisms exist to protect external and internal wireless links from signal parameter attacks through monitoring for unauthorized wireless connections, including scanning for unauthorized wireless access points and taking appropriate action, if an unauthorized connection is discovered.	5		Not Selected
SC-40	Wireless Link Protection	Protect external and internal [Assignment: organization-defined wireless links] from the following signal parameter attacks: [Assignment: organization-defined types of signal parameter attacks or references to sources for such attacks].	Functional	Intersects With	Wireless Access Authentication & Encryption	CRY-07	Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption.	5		Not Selected
SC-40(01)	Wireless Link Protection | Electromagnetic Interference	Implement cryptographic mechanisms that achieve [Assignment: organization-defined level of protection] against the effects of intentional electromagnetic interference.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SC-40(02)	Wireless Link Protection | Reduce Detection Potential	Implement cryptographic mechanisms to reduce the detection potential of wireless links to [Assignment: organization-defined level of reduction].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SC-40(03)	Wireless Link Protection | Imitative or Manipulative Communications Deception	Implement cryptographic mechanisms to identify and reject wireless transmissions that are deliberate attempts to achieve imitative or manipulative communications deception based on signal parameters.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SC-40(04)	Wireless Link Protection | Signal Parameter Identification	Implement cryptographic mechanisms to prevent the identification of [Assignment: organization-defined wireless transmitters] by using the transmitter signal parameters.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SC-41	Port and I/O Device Access	[Selection (one): Physically; Logically] disable or remove [Assignment: organization-defined connection ports or input/output devices] on the following systems or system components: [Assignment: organization-defined systems or system components].	Functional	Equal	Port & Input / Output (I/O) Device Access	END-12	Mechanisms exist to physically disable or remove unnecessary connection ports or input/output devices from sensitive systems.	10		Not Selected
SC-42	Sensor Capability and Data	a. Prohibit [Selection (one or more): the use of devices possessing [Assignment: organization-defined environmental sensing capabilities] in [Assignment: organization-defined facilities, areas, or systems]; the remote activation of environmental sensing capabilities on organizational systems or system components with the following exceptions: [Assignment: organization-defined exceptions where remote activation of sensors is allowed]]; andb. Provide an explicit indication of sensor use to [Assignment: organization-defined group of users].	Functional	Equal	Sensor Capability	END-13	Mechanisms exist to configure embedded sensors on systems to: (1) Prohibit the remote activation of sensing capabilities; and (2) Provide an explicit indication of sensor use to users.	10		Not Selected
SC-42(01)	Sensor Capability and Data | Reporting to Authorized Individuals or Roles	Verify that the system is configured so that data or information collected by the [Assignment: organization-defined sensors] is only reported to authorized individuals or roles.	Functional	Equal	Sensor Delivery Verification	END-13.4	Mechanisms exist to verify embedded technology sensors are configured so that data collected by the sensor(s) is only reported to authorized individuals or roles.	10		Not Selected
SC-42(02)	Sensor Capability and Data | Authorized Use	Employ the following measures so that data or information collected by [Assignment: organization-defined sensors] is only used for authorized purposes: [Assignment: organization-defined measures].	Functional	Equal	Authorized Use	END-13.1	Mechanisms exist to utilize organization-defined measures so that data or information collected by sensors is only used for authorized purposes.	10		Not Selected
SC-42(03)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SC-42(04)	Sensor Capability and Data | Notice of Collection	Employ the following measures to facilitate an individual's awareness that personally identifiable information is being collected by [Assignment: organization-defined sensors]: [Assignment: organization-defined measures].	Functional	Equal	Notice of Collection	END-13.2	Mechanisms exist to notify individuals that Personal Data (PD) is collected by sensors.	10		Not Selected
SC-42(05)	Sensor Capability and Data | Collection Minimization	Employ [Assignment: organization-defined sensors] that are configured to minimize the collection of information about individuals that is not needed.	Functional	Equal	Collection Minimization	END-13.3	Mechanisms exist to utilize sensors that are configured to minimize the collection of information about individuals.	10		Not Selected
SC-43	Usage Restrictions	a. Establish usage restrictions and implementation guidelines for the following system components: [Assignment: organization-defined system components]; andb. Authorize, monitor, and control the use of such components within the system.	Functional	Equal	Usage Parameters	AST-14	Mechanisms exist to monitor and enforce usage parameters that limit the potential damage caused from the unauthorized or unintentional alteration of system parameters.	10		Not Selected
SC-44	Detonation Chambers	Employ a detonation chamber capability within [Assignment: organization-defined system, system component, or location].	Functional	Equal	Detonation Chambers (Sandboxes)	IRO-15	Mechanisms exist to utilize a detonation chamber capability to detect and/or block potentially-malicious files and email attachments.	10		Not Selected
SC-45	System Time Synchronization	Synchronize system clocks within and between systems and system components.	Functional	Intersects With	Synchronization With Authoritative Time Source	MON-07.1	Mechanisms exist to synchronize internal system clocks with an authoritative time source.	5		Not Selected
SC-45(01)	System Time Synchronization | Synchronization with Authoritative Time Source	a. Compare the internal system clocks [Assignment: organization-defined frequency] with [Assignment: organization-defined authoritative time source]; andb. Synchronize the internal system clocks to the authoritative time source when the time difference is greater than [Assignment: organization-defined time period].	Functional	Equal	Synchronization With Authoritative Time Source	MON-07.1	Mechanisms exist to synchronize internal system clocks with an authoritative time source.	10		Not Selected
SC-45(02)	System Time Synchronization | Secondary Authoritative Time Source	a. Identify a secondary authoritative time source that is in a different geographic region than the primary authoritative time source; andb. Synchronize the internal system clocks to the secondary authoritative time source if the primary authoritative time source is unavailable.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SC-46	Cross Domain Policy Enforcement	Implement a policy enforcement mechanism [Selection (one): physically; logically] between the physical and/or network interfaces for the connecting security domains.	Functional	Equal	Cross Domain Solution (CDS)	NET-02.3	Mechanisms exist to implement a Cross Domain Solution (CDS) to mitigate the specific security risks of accessing or transferring information between security domains.	10		Not Selected
SC-47	Alternate Communications Channels	Establish [Assignment: organization-defined alternate communications paths] for system operations organizational command and control.	Functional	Equal	Alternate Communications Channels	BCD-10.4	Mechanisms exist to maintain command and control capabilities via alternate communications channels and designating alternative decision makers if primary decision makers are unavailable.	10		Not Selected
SC-48	Sensor Relocation	Relocate [Assignment: organization-defined sensors and monitoring capabilities] to [Assignment: organization-defined locations] under the following conditions or circumstances: [Assignment: organization-defined conditions or circumstances].	Functional	Intersects With	Threat Hunting	THR-07	Mechanisms exist to perform cyber threat hunting that uses Indicators of Compromise (IoC) to detect, track and disrupt threats that evade existing security controls.	5		Not Selected
SC-48	Sensor Relocation	Relocate [Assignment: organization-defined sensors and monitoring capabilities] to [Assignment: organization-defined locations] under the following conditions or circumstances: [Assignment: organization-defined conditions or circumstances].	Functional	Intersects With	Automated Tools for Real-Time Analysis	MON-01.2	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support near real-time analysis and incident escalation.	5		Not Selected
SC-48(01)	Sensor Relocation | Dynamic Relocation of Sensors or Monitoring Capabilities	Dynamically relocate [Assignment: organization-defined sensors and monitoring capabilities] to [Assignment: organization-defined locations] under the following conditions or circumstances: [Assignment: organization-defined conditions or circumstances].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SC-49	Hardware-enforced Separation and Policy Enforcement	Implement hardware-enforced separation and policy enforcement mechanisms between [Assignment: organization-defined security domains].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SC-50	Software-enforced Separation and Policy Enforcement	Implement software-enforced separation and policy enforcement mechanisms between [Assignment: organization-defined security domains].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-53B Baseline
SC-51	Hardware-based Protection	a. Employ hardware-based, write-protect for [Assignment: organization-defined system firmware components]; andb. Implement specific procedures for [Assignment: organization-defined authorized individuals] to manually disable hardware write-protect for firmware modifications and re-enable the write-protect prior to returning to operational mode.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SI-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and information integrity policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and information integrity policy and procedures; andc. Review and update the current system and information integrity:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5		Low
SI-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and information integrity policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and information integrity policy and procedures; andc. Review and update the current system and information integrity:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	10		Low
SI-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and information integrity policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and information integrity policy and procedures; andc. Review and update the current system and information integrity:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5		Low
SI-02	Flaw Remediation	a. Identify, report, and correct system flaws;b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;c. Install security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates; andd. Incorporate flaw remediation into the organizational configuration management process.	Functional	Intersects With	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	5		Low
SI-02	Flaw Remediation	a. Identify, report, and correct system flaws;b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;c. Install security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates; andd. Incorporate flaw remediation into the organizational configuration management process.	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5		Low
SI-02	Flaw Remediation	a. Identify, report, and correct system flaws;b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;c. Install security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates; andd. Incorporate flaw remediation into the organizational configuration management process.	Functional	Intersects With	Automatic Antimalware Signature Updates	END-04.1	Automated mechanisms exist to update antimalware technologies, including signature definitions.	5		Low
SI-02(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SI-02(02)	Flaw Remediation | Automated Flaw Remediation Status	Determine if system components have applicable security-relevant software and firmware updates installed using [Assignment: organization-defined automated mechanisms] [Assignment: organization-defined frequency].	Functional	Intersects With	Automated Remediation Status	VPM-05.2	Automated mechanisms exist to determine the state of system components with regard to flaw remediation.	5		Moderate
SI-02(03)	Flaw Remediation | Time to Remediate Flaws and Benchmarks for Corrective Actions	a. Measure the time between flaw identification and flaw remediation; andb. Establish the following benchmarks for taking corrective actions: [Assignment: organization-defined benchmarks].	Functional	Equal	Time To Remediate / Benchmarks For Corrective Action	VPM-05.3	Mechanisms exist to track the effectiveness of remediation operations through metrics reporting.	10		Not Selected
SI-02(04)	Flaw Remediation | Automated Patch Management Tools	Employ automated patch management tools to facilitate flaw remediation to the following system components: [Assignment: organization-defined system components].	Functional	Intersects With	Automated Remediation Status	VPM-05.2	Automated mechanisms exist to determine the state of system components with regard to flaw remediation.	5		Not Selected
SI-02(04)	Flaw Remediation | Automated Patch Management Tools	Employ automated patch management tools to facilitate flaw remediation to the following system components: [Assignment: organization-defined system components].	Functional	Intersects With	Automated Software & Firmware Updates	VPM-05.4	Automated mechanisms exist to install the latest stable versions of security-relevant software and firmware updates.	5		Not Selected
SI-02(04)	Flaw Remediation | Automated Patch Management Tools	Employ automated patch management tools to facilitate flaw remediation to the following system components: [Assignment: organization-defined system components].	Functional	Intersects With	Centralized Management of Flaw Remediation Processes	VPM-05.1	Mechanisms exist to centrally-manage the flaw remediation process.	5		Not Selected
SI-02(04)	Flaw Remediation | Automated Patch Management Tools	Employ automated patch management tools to facilitate flaw remediation to the following system components: [Assignment: organization-defined system components].	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5		Not Selected
SI-02(05)	Flaw Remediation | Automatic Software and Firmware Updates	Install [Assignment: organization-defined security-relevant software and firmware updates] automatically to [Assignment: organization-defined system components].	Functional	Intersects With	Automated Software & Firmware Updates	VPM-05.4	Automated mechanisms exist to install the latest stable versions of security-relevant software and firmware updates.	5		Not Selected
SI-02(06)	Flaw Remediation | Removal of Previous Versions of Software and Firmware	Remove previous versions of [Assignment: organization-defined software and firmware components] after updated versions have been installed.	Functional	Equal	Removal of Previous Versions	VPM-05.5	Mechanisms exist to remove old versions of software and firmware components after updated versions have been installed.	10		Not Selected

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh	Notes	NIST SP 800-53B Baseline
SI-02(07)	Flaw Remediation | Root Cause Analysis	a. Conduct root cause analysis to identify the underlying causes of issues or failures; b. Develop actions to address the root cause of the issue or failure; c. Implement the actions and monitor the implementation for effectiveness.	Functional	Equal	Software Design Root Cause Analysis	TDA-06.6	Mechanisms exist to assess software design processes that includes: (1) Conducting Root Cause Analysis (RCA) to identify the underlying causes of issues or failures; (2) Developing actions to address the root cause of the issue or failure; and (3) Implementing the actions and monitoring the implementation	10		Not Selected
SI-03	Malicious Code Protection	a. Implement [Selection (one or more): signature based; non-signature based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;c. Configure malicious code protection mechanisms to:1. Perform periodic scans of the system [Assignment: organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more): endpoint; network entry and exit points] as the files are downloaded, opened, or executed in accordance with organizational policy; and2. [Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]; and send alert to [Assignment: organization-defined personnel or roles] in response to malicious code detection; andd. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5		Low
SI-03	Malicious Code Protection	a. Implement [Selection (one or more): signature based; non-signature based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;c. Configure malicious code protection mechanisms to:1. Perform periodic scans of the system [Assignment: organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more): endpoint; network entry and exit points] as the files are downloaded, opened, or executed in accordance with organizational policy; and2. [Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]; and send alert to [Assignment: organization-defined personnel or roles] in response to malicious code detection; andd. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.	Functional	Intersects With	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	5		Low
SI-03	Malicious Code Protection	a. Implement [Selection (one or more): signature based; non-signature based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;c. Configure malicious code protection mechanisms to:1. Perform periodic scans of the system [Assignment: organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more): endpoint; network entry and exit points] as the files are downloaded, opened, or executed in accordance with organizational policy; and2. [Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]; and send alert to [Assignment: organization-defined personnel or roles] in response to malicious code detection; andd. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	5		Low
SI-03	Malicious Code Protection	a. Implement [Selection (one or more): signature based; non-signature based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;c. Configure malicious code protection mechanisms to:1. Perform periodic scans of the system [Assignment: organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more): endpoint; network entry and exit points] as the files are downloaded, opened, or executed in accordance with organizational policy; and2. [Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]; and send alert to [Assignment: organization-defined personnel or roles] in response to malicious code detection; andd. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.	Functional	Intersects With	Heuristic / Nonsignature-Based Detection	END-04.4	Mechanisms exist to utilize heuristic / nonsignature-based antimalware detection capabilities.	5		Low
SI-03	Malicious Code Protection	a. Implement [Selection (one or more): signature based; non-signature based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;c. Configure malicious code protection mechanisms to:1. Perform periodic scans of the system [Assignment: organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more): endpoint; network entry and exit points] as the files are downloaded, opened, or executed in accordance with organizational policy; and2. [Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]; and send alert to [Assignment: organization-defined personnel or roles] in response to malicious code detection; andd. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-12	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.	5		Low
SI-03	Malicious Code Protection	a. Implement [Selection (one or more): signature based; non-signature based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;c. Configure malicious code protection mechanisms to:1. Perform periodic scans of the system [Assignment: organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more): endpoint; network entry and exit points] as the files are downloaded, opened, or executed in accordance with organizational policy; and2. [Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]; and send alert to [Assignment: organization-defined personnel or roles] in response to malicious code detection; andd. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.	Functional	Intersects With	Automatic Antimalware Signature Updates	END-04.1	Automated mechanisms exist to update antimalware technologies, including signature definitions.	5		Low

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-53B Baseline
SI-03	Malicious Code Protection	a. Implement [Selection (one or more): signature based; non-signature based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;c. Configure malicious code protection mechanisms to:1. Perform periodic scans of the system [Assignment: organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more): endpoint; network entry and exit points] as the files are downloaded, opened, or executed in accordance with organizational policy; and2. [Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]; and send alert to [Assignment: organization-defined personnel or roles] in response to malicious code detection; andd. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5		Low
SI-03(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SI-03(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SI-03(03)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SI-03(04)	Malicious Code Protection | Updates Only by Privileged Users	Update malicious code protection mechanisms only when directed by a privileged user.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SI-03(05)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SI-03(06)	Malicious Code Protection | Testing and Verification	a. Test malicious code protection mechanisms [Assignment: organization-defined frequency] by introducing known benign code into the system; andb. Verify that the detection of the code and the associated incident reporting occur.	Functional	Equal	Malware Protection Mechanism Testing	END-04.5	Mechanisms exist to test antimalware technologies by introducing a known benign, non-spreading test case into the system and subsequently verifying that both detection of the test case and associated incident reporting occurs.	10		Not Selected
SI-03(07)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SI-03(08)	Malicious Code Protection | Detect Unauthorized Commands	a. Detect the following unauthorized operating system commands through the kernel application programming interface on [Assignment: organization-defined system hardware components]: [Assignment: organization-defined unauthorized operating system commands]; andb. [Selection (one or more): issue a warning; audit the command execution; prevent the execution of the command].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SI-03(09)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SI-03(10)	Malicious Code Protection | Malicious Code Analysis	a. Employ the following tools and techniques to analyze the characteristics and behavior of malicious code: [Assignment: organization-defined tools and techniques]; andb. Incorporate the results from malicious code analysis into organizational incident response and flaw remediation processes.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SI-04	System Monitoring	a. Monitor the system to detect:1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]; and2. Unauthorized local, network, and remote connections;b. Identify unauthorized use of the system through the following techniques and methods: [Assignment: organization-defined techniques and methods];c. Invoke internal monitoring capabilities or deploy monitoring devices:1. Strategically within the system to collect organization-determined essential information; and2. At ad hoc locations within the system to track specific types of transactions of interest to the organization;d. Analyze detected events and anomalies;e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation;f. Obtain legal opinion regarding system monitoring activities; andg. Provide [Assignment: organization-defined system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5		Low
SI-04	System Monitoring	a. Monitor the system to detect:1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]; and2. Unauthorized local, network, and remote connections;b. Identify unauthorized use of the system through the following techniques and methods: [Assignment: organization-defined techniques and methods];c. Invoke internal monitoring capabilities or deploy monitoring devices:1. Strategically within the system to collect organization-determined essential information; and2. At ad hoc locations within the system to track specific types of transactions of interest to the organization;d. Analyze detected events and anomalies;e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation;f. Obtain legal opinion regarding system monitoring activities; andg. Provide [Assignment: organization-defined system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	5		Low
SI-04	System Monitoring	a. Monitor the system to detect:1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]; and2. Unauthorized local, network, and remote connections;b. Identify unauthorized use of the system through the following techniques and methods: [Assignment: organization-defined techniques and methods];c. Invoke internal monitoring capabilities or deploy monitoring devices:1. Strategically within the system to collect organization-determined essential information; and2. At ad hoc locations within the system to track specific types of transactions of interest to the organization;d. Analyze detected events and anomalies;e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation;f. Obtain legal opinion regarding system monitoring activities; andg. Provide [Assignment: organization-defined system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-12	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.	5		Low

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-53B Baseline
SI-04	System Monitoring	a. Monitor the system to detect:1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]; and2. Unauthorized local, network, and remote connections;b. Identify unauthorized use of the system through the following techniques and methods: [Assignment: organization-defined techniques and methods];c. Invoke internal monitoring capabilities or deploy monitoring devices:1. Strategically within the system to collect organization-determined essential information; and2. At ad hoc locations within the system to track specific types of transactions of interest to the organization;d. Analyze detected events and anomalies;e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation;f. Obtain legal opinion regarding system monitoring activities; andg. Provide [Assignment: organization-defined system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].	Functional	Intersects With	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	5		Low
SI-04(01)	System Monitoring | System-wide Intrusion Detection System	Connect and configure individual intrusion detection tools into a system-wide intrusion detection system.	Functional	Equal	Intrusion Detection & Prevention Systems (IDS & IPS)	MON-01.1	Mechanisms exist to implement Intrusion Detection / Prevention Systems (IDS / IPS) technologies on critical systems, key network segments and network choke points.	10		Not Selected
SI-04(02)	System Monitoring | Automated Tools and Mechanisms for Real-time Analysis	Employ automated tools and mechanisms to support near real-time analysis of events.	Functional	Equal	Automated Tools for Real-Time Analysis	MON-01.2	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support near real-time analysis and incident escalation.	10		Moderate
SI-04(03)	System Monitoring | Automated Tool and Mechanism Integration	Employ automated tools and mechanisms to integrate intrusion detection tools and mechanisms into access control and flow control mechanisms.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SI-04(04)	System Monitoring | Inbound and Outbound Communications Traffic	a. Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic;b. Monitor inbound and outbound communications traffic [Assignment: organization-defined frequency] for [Assignment: organization-defined unusual or unauthorized activities or conditions].	Functional	Equal	Inbound & Outbound Communications Traffic	MON-01.3	Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.	10		Moderate
SI-04(05)	System Monitoring | System-generated Alerts	Alert [Assignment: organization-defined personnel or roles] when the following system-generated indications of compromise or potential compromise occur: [Assignment: organization-defined compromise indicators].	Functional	Equal	System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data protection and supply chain activities to achieve integrated situational awareness.	10		Moderate
SI-04(06)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SI-04(07)	System Monitoring | Automated Response to Suspicious Events	a. Notify [Assignment: organization-defined incident response personnel (identified by name and/or by role)] of detected suspicious events; andb. Take the following actions upon detection: [Assignment: organization-defined least-disruptive actions to terminate suspicious events].	Functional	Intersects With	Automated Response to Suspicious Events	MON-01.11	Automated mechanisms exist to implement pre-determined corrective actions in response to detected events that have security incident implications.	5		Not Selected
SI-04(07)	System Monitoring | Automated Response to Suspicious Events	a. Notify [Assignment: organization-defined incident response personnel (identified by name and/or by role)] of detected suspicious events; andb. Take the following actions upon detection: [Assignment: organization-defined least-disruptive actions to terminate suspicious events].	Functional	Intersects With	Automated Incident Handling Processes	IRO-02.1	Automated mechanisms exist to support the incident handling process.	5		Not Selected
SI-04(08)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SI-04(09)	System Monitoring | Testing of Monitoring Tools and Mechanisms	Test intrusion-monitoring tools and mechanisms [Assignment: organization-defined frequency].	Functional	Intersects With	Incident Response Testing	IRO-06	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	5		Not Selected
SI-04(10)	System Monitoring | Visibility of Encrypted Communications	Make provisions so that [Assignment: organization-defined encrypted communications traffic] is visible to [Assignment: organization-defined system monitoring tools and mechanisms].	Functional	Equal	Visibility of Encrypted Communications	NET-18.2	Mechanisms exist to configure the proxy to make encrypted communications traffic visible to monitoring tools and mechanisms.	10		High
SI-04(11)	System Monitoring | Analyze Communications Traffic Anomalies	Analyze outbound communications traffic at the external interfaces to the system and selected [Assignment: organization-defined interior points within the system] to discover anomalies.	Functional	Equal	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	10		Not Selected
SI-04(12)	System Monitoring | Automated Organization-generated Alerts	Alert [Assignment: organization-defined personnel or roles] using [Assignment: organization-defined automated mechanisms] when the following indications of inappropriate or unusual activities with security or privacy implications occur: [Assignment: organization-defined activities that trigger alerts].	Functional	Intersects With	Automated Alerts	MON-01.12	Mechanisms exist to automatically alert incident response personnel to inappropriate or anomalous activities that have potential security incident implications.	5		High
SI-04(12)	System Monitoring | Automated Organization-generated Alerts	Alert [Assignment: organization-defined personnel or roles] using [Assignment: organization-defined automated mechanisms] when the following indications of inappropriate or unusual activities with security or privacy implications occur: [Assignment: organization-defined activities that trigger alerts].	Functional	Intersects With	Real-Time Alerts of Event Logging Failure	MON-05.1	Mechanisms exist to provide 24x7x365 near real-time alerting capability when an event log processing failure occurs.	5		High
SI-04(13)	System Monitoring | Analyze Traffic and Event Patterns	a. Analyze communications traffic and event patterns for the system;b. Develop profiles representing common traffic and event patterns; andc. Use the traffic and event profiles in tuning system-monitoring devices.	Functional	Equal	Alert Threshold Tuning	MON-01.13	Mechanisms exist to "tune" event monitoring technologies through analyzing communications traffic/event patterns and developing profiles representing common traffic patterns and/or events.	10		Not Selected
SI-04(14)	System Monitoring | Wireless Intrusion Detection	Employ a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises or breaches to the system.	Functional	Intersects With	Wireless Network Monitoring	MON-01.5	Mechanisms exist to monitor wireless network segments for: (1) Rogue wireless devices; and (2) Anomalous and/or hostile activities.	5		High
SI-04(15)	System Monitoring | Wireless to Wireline Communications	Employ an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wireline networks.	Functional	Intersects With	Wireless Intrusion Detection / Prevention Systems (WIDS / WIPS) Deployment	NET-08.2	Mechanisms exist to utilize Wireless Intrusion Detection / Protection Systems (WIDS / WIPS) on wireless network segments.	5		Not Selected
SI-04(16)	System Monitoring | Correlate Monitoring Information	Correlate information from monitoring tools and mechanisms employed throughout the system.	Functional	Equal	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.	10		Not Selected
SI-04(17)	System Monitoring | Integrated Situational Awareness	Correlate information from monitoring physical, cyber, and supply chain activities to achieve integrated, organization-wide situational awareness.	Functional	Equal	Integration of Scanning & Other Monitoring Information	MON-02.3	Automated mechanisms exist to integrate the analysis of audit records with analysis of vulnerability scanners, network performance, system monitoring and other sources to further enhance the ability to identify inappropriate or unusual activity.	10		Not Selected
SI-04(18)	System Monitoring | Analyze Traffic and Covert Exfiltration	Analyze outbound communications traffic at external interfaces to the system and at the following interior points to detect covert exfiltration of information: [Assignment: organization-defined interior points within the system].	Functional	Intersects With	Data Loss Prevention (DLP)	NET-17	Automated mechanisms exist to implement Data Loss Prevention (DLP) to protect sensitive information as it is stored, transmitted and processed.	5		Not Selected
SI-04(18)	System Monitoring | Analyze Traffic and Covert Exfiltration	Analyze outbound communications traffic at external interfaces to the system and at the following interior points to detect covert exfiltration of information: [Assignment: organization-defined interior points within the system].	Functional	Intersects With	Analyze Traffic for Covert Exfiltration	MON-11.1	Automated mechanisms exist to analyze network traffic to detect covert data exfiltration.	5		Not Selected
SI-04(19)	System Monitoring | Risk for Individuals	Implement [Assignment: organization-defined additional monitoring] of individuals who have been identified by [Assignment: organization-defined sources] as posing an increased level of risk.	Functional	Equal	Individuals Posing Greater Risk	MON-01.14	Mechanisms exist to implement enhanced activity monitoring for individuals who have been identified as posing an increased level of risk.	10		Not Selected

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-53B Baseline
SI-04(20)	System Monitoring | Privileged Users	Implement the following additional monitoring of privileged users: [Assignment: organization-defined additional monitoring].	Functional	Equal	Privileged User Oversight	MON-01.15	Mechanisms exist to implement enhanced activity monitoring for privileged users.	10		High
SI-04(21)	System Monitoring | Probationary Periods	Implement the following additional monitoring of individuals during [Assignment: organization-defined probationary period]: [Assignment: organization-defined additional monitoring].	Functional	Equal	Probationary Periods	HRS-02.2	Mechanisms exist to identify newly onboarded personnel for enhanced monitoring during their probationary period.	10		Not Selected
SI-04(22)	System Monitoring | Unauthorized Network Services	a. Detect network services that have not been authorized or approved by [Assignment: organization-defined authorization or approval processes]; andb. [Selection (one or more): Audit; Alert [Assignment: organization-defined personnel or roles]] when detected.	Functional	Equal	Unauthorized Network Services	MON-11.2	Automated mechanisms exist to detect unauthorized network services and alert incident response personnel.	10		High
SI-04(23)	System Monitoring | Host-based Devices	Implement the following host-based monitoring mechanisms at [Assignment: organization-defined system components]: [Assignment: organization-defined host-based monitoring mechanisms].	Functional	Equal	Host-Based Devices	MON-01.6	Mechanisms exist to utilize Host-based Intrusion Detection / Prevention Systems (HIDS / HIPS) to actively alert on or block unwanted activities and send logs to a Security Incident Event Manager (SIEM), or similar automated tool, to maintain situational awareness.	10		Not Selected
SI-04(24)	System Monitoring | Indicators of Compromise	Discover, collect, and distribute to [Assignment: organization-defined personnel or roles], indicators of compromise provided by [Assignment: organization-defined sources].	Functional	Intersects With	Monitoring for Indicators of Compromise (IOC)	MON-11.3	Automated mechanisms exist to identify and alert on Indicators of Compromise (IoC).	5		Not Selected
SI-04(24)	System Monitoring | Indicators of Compromise	Discover, collect, and distribute to [Assignment: organization-defined personnel or roles], indicators of compromise provided by [Assignment: organization-defined sources].	Functional	Intersects With	File Integrity Monitoring (FIM)	MON-01.7	Mechanisms exist to utilize a File Integrity Monitor (FIM), or similar change-detection technology, on critical Technology Assets, Applications and/or Services (TAAS) to generate alerts for unauthorized modifications.	5		Not Selected
SI-04(25)	System Monitoring | Optimize Network Traffic Analysis	Provide visibility into network traffic at external and key internal system interfaces to optimize the effectiveness of monitoring devices.	Functional	Intersects With	Limit Network Connections	NET-03.1	Mechanisms exist to limit the number of concurrent external network connections to its Technology Assets, Applications and/or Services (TAAS).	5		Not Selected
SI-04(25)	System Monitoring | Optimize Network Traffic Analysis	Provide visibility into network traffic at external and key internal system interfaces to optimize the effectiveness of monitoring devices.	Functional	Intersects With	Intrusion Detection & Prevention Systems (IDS & IPS)	MON-01.1	Mechanisms exist to implement Intrusion Detection / Prevention Systems (IDS / IPS) technologies on critical systems, key network segments and network choke points.	5		Not Selected
SI-05	Security Alerts, Advisories, and Directives	a. Receive system security alerts, advisories, and directives from [Assignment: organization-defined external organizations] on an ongoing basis;b. Generate internal security alerts, advisories, and directives as deemed necessary;c. Disseminate security alerts, advisories, and directives to: [Selection (one or more): [Assignment: organization-defined personnel or roles]; [Assignment: organization-defined elements within the organization]; [Assignment: organization-defined external organizations]]; andd. Implement security directives in accordance with established time frames, or notify the issuing organization of the degree of noncompliance.	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5		Low
SI-05	Security Alerts, Advisories, and Directives	a. Receive system security alerts, advisories, and directives from [Assignment: organization-defined external organizations] on an ongoing basis;b. Generate internal security alerts, advisories, and directives as deemed necessary;c. Disseminate security alerts, advisories, and directives to: [Selection (one or more): [Assignment: organization-defined personnel or roles]; [Assignment: organization-defined elements within the organization]; [Assignment: organization-defined external organizations]]; andd. Implement security directives in accordance with established time frames, or notify the issuing organization of the degree of noncompliance.	Functional	Intersects With	Threat Intelligence Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5		Low
SI-05	Security Alerts, Advisories, and Directives	a. Receive system security alerts, advisories, and directives from [Assignment: organization-defined external organizations] on an ongoing basis;b. Generate internal security alerts, advisories, and directives as deemed necessary;c. Disseminate security alerts, advisories, and directives to: [Selection (one or more): [Assignment: organization-defined personnel or roles]; [Assignment: organization-defined elements within the organization]; [Assignment: organization-defined external organizations]]; andd. Implement security directives in accordance with established time frames, or notify the issuing organization of the degree of noncompliance.	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-12	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.	5		Low
SI-05(01)	Security Alerts, Advisories, and Directives | Automated Alerts and Advisories	Broadcast security alert and advisory information throughout the organization using [Assignment: organization-defined automated mechanisms].	Functional	Intersects With	Threat Intelligence Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5		High
SI-06	Security and Privacy Function Verification	a. Verify the correct operation of [Assignment: organization-defined security and privacy functions];b. Perform the verification of the functions specified in SI-06a [Selection (one or more): [Assignment: organization-defined system transitional states]; upon command by user with appropriate privilege; [Assignment: organization-defined frequency]];c. Alert [Assignment: organization-defined personnel or roles] to failed security and privacy verification tests; andd. [Selection (one or more): Shut the system down; Restart the system; [Assignment: organization-defined alternative action(s)]] when anomalies are discovered.	Functional	Intersects With	Control Functionality Verification	CHG-06	Mechanisms exist to verify the functionality of security, compliance and resilience controls following implemented changes to ensure applicable controls operate as designed.	5		High
SI-06(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SI-06(02)	Security and Privacy Function Verification | Automation Support for Distributed Testing	Implement automated mechanisms to support the management of distributed security and privacy function testing.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SI-06(03)	Security and Privacy Function Verification | Report Verification Results	Report the results of security and privacy function verification to [Assignment: organization-defined personnel or roles].	Functional	Equal	Report Verification Results	CHG-06.1	Mechanisms exist to report the results of security, compliance and resilience capability verification to appropriate organizational management.	10		Not Selected
SI-07	Software, Firmware, and Information Integrity	a. Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: [Assignment: organization-defined software, firmware, and information]; andb. Take the following actions when unauthorized changes to the software, firmware, and information are detected: [Assignment: organization-defined actions].	Functional	Intersects With	Endpoint File Integrity Monitoring (FIM)	END-06	Mechanisms exist to utilize File Integrity Monitor (FIM), or similar technologies, to detect and report on unauthorized changes to selected files and configuration settings.	5		Moderate
SI-07	Software, Firmware, and Information Integrity	a. Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: [Assignment: organization-defined software, firmware, and information]; andb. Take the following actions when unauthorized changes to the software, firmware, and information are detected: [Assignment: organization-defined actions].	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-12	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.	5		Moderate
SI-07	Software, Firmware, and Information Integrity	a. Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: [Assignment: organization-defined software, firmware, and information]; andb. Take the following actions when unauthorized changes to the software, firmware, and information are detected: [Assignment: organization-defined actions].	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5		Moderate
SI-07(01)	Software, Firmware, and Information Integrity | Integrity Checks	Perform an integrity check of [Assignment: organization-defined software, firmware, and information] [Selection (one or more): at startup; at [Assignment: organization-defined transitional states or security-relevant events]; [Assignment: organization-defined frequency]].	Functional	Equal	Integrity Checks	END-06.1	Mechanisms exist to validate configurations through integrity checking of software and firmware.	10		Moderate
SI-07(02)	Software, Firmware, and Information Integrity | Automated Notifications of Integrity Violations	Employ automated tools that provide notification to [Assignment: organization-defined personnel or roles] upon discovering discrepancies during integrity verification.	Functional	Equal	Automated Notifications of Integrity Violations	END-06.3	Automated mechanisms exist to alert incident response personnel upon discovering discrepancies during integrity verification.	10		High

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-53B Baseline
SI-07(03)	Software, Firmware, and Information Integrity | Centrally Managed Integrity Tools	Employ centrally managed integrity verification tools.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SI-07(04)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SI-07(05)	Software, Firmware, and Information Integrity | Automated Response to Integrity Violations	Automatically [Selection (one or more): shut the system down; restart the system; implement [Assignment: organization-defined controls]] when integrity violations are discovered.	Functional	Equal	Automated Response to Integrity Violations	END-06.4	Automated mechanisms exist to implement remediation actions when integrity violations are discovered.	10		High
SI-07(06)	Software, Firmware, and Information Integrity | Cryptographic Protection	Implement cryptographic mechanisms to detect unauthorized changes to software, firmware, and information.	Functional	Equal	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10		Not Selected
SI-07(07)	Software, Firmware, and Information Integrity | Integration of Detection and Response	Incorporate the detection of the following unauthorized changes into the organizational incident response capability: [Assignment: organization-defined security-relevant changes to the system].	Functional	Equal	Endpoint Detection & Response (EDR)	END-06.2	Mechanisms exist to detect and respond to unauthorized configuration changes as cybersecurity incidents.	10		Moderate
SI-07(08)	Software, Firmware, and Information Integrity | Auditing Capability for Significant Events	Upon detection of a potential integrity violation, provide the capability to audit the event and initiate the following actions: [Selection (one or more): generate an audit record; alert current user; alert [Assignment: organization-defined personnel or roles]; [Assignment: organization-defined other actions]].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SI-07(09)	Software, Firmware, and Information Integrity | Verify Boot Process	Verify the integrity of the boot process of the following system components: [Assignment: organization-defined system components].	Functional	Equal	Boot Process Integrity	END-06.5	Automated mechanisms exist to verify the integrity of the boot process of systems.	10		Not Selected
SI-07(10)	Software, Firmware, and Information Integrity | Protection of Boot Firmware	Implement the following mechanisms to protect the integrity of boot firmware in [Assignment: organization-defined system components]: [Assignment: organization-defined mechanisms].	Functional	Equal	Protection of Boot Firmware	END-06.6	Automated mechanisms exist to protect the integrity of boot firmware in systems.	10		Not Selected
SI-07(11)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SI-07(12)	Software, Firmware, and Information Integrity | Integrity Verification	Require that the integrity of the following user-installed software be verified prior to execution: [Assignment: organization-defined user-installed software].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SI-07(13)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SI-07(14)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SI-07(15)	Software, Firmware, and Information Integrity | Code Authentication	Implement cryptographic mechanisms to authenticate the following software or firmware components prior to installation: [Assignment: organization-defined software or firmware components].	Functional	Intersects With	Signed Components	CHG-04.2	Mechanisms exist to prevent the installation of software and firmware components without verification that the component has been digitally signed using an organization-approved certificate authority.	5		High
SI-07(16)	Software, Firmware, and Information Integrity | Time Limit on Process Execution Without Supervision	Prohibit processes from executing without supervision for more than [Assignment: organization-defined time period].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SI-07(17)	Software, Firmware, and Information Integrity | Runtime Application Self-protection	Implement [Assignment: organization-defined controls] for application self-protection at runtime.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SI-08	Spam Protection	a. Employ spam protection mechanisms at system entry and exit points to detect and act on unsolicited messages; andb. Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.	Functional	Equal	Phishing & Spam Protection	END-08	Mechanisms exist to utilize anti-phishing and spam protection technologies to detect and take action on unsolicited messages transported by electronic mail.	10		Moderate
SI-08(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SI-08(02)	Spam Protection | Automatic Updates	Automatically update spam protection mechanisms [Assignment: organization-defined frequency].	Functional	Equal	Automatic Spam and Phishing Protection Updates	END-08.2	Mechanisms exist to automatically update anti-phishing and spam protection technologies when new releases are available in accordance with configuration and change management practices.	10		Moderate
SI-08(03)	Spam Protection | Continuous Learning Capability	Implement spam protection mechanisms with a learning capability to more effectively identify legitimate communications traffic.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SI-09		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SI-10	Information Input Validation	Check the validity of the following information inputs: [Assignment: organization-defined information inputs to the system].	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-12	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.	5		Moderate
SI-10	Information Input Validation	Check the validity of the following information inputs: [Assignment: organization-defined information inputs to the system].	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5		Moderate
SI-10(01)	Information Input Validation | Manual Override Capability	a. Provide a manual override capability for input validation of the following information inputs: [Assignment: organization-defined inputs defined in the base control (SI-10)];b. Restrict the use of the manual override capability to only [Assignment: organization-defined authorized individuals]; andc. Audit the use of the manual override capability.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SI-10(02)	Information Input Validation | Review and Resolve Errors	Review and resolve input validation errors within [Assignment: organization-defined time period].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SI-10(03)	Information Input Validation | Predictable Behavior	Verify that the system behaves in a predictable and documented manner when invalid inputs are received.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SI-10(04)	Information Input Validation | Timing Interactions	Account for timing interactions among system components in determining appropriate responses for invalid inputs.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SI-10(05)	Information Input Validation | Restrict Inputs to Trusted Sources and Approved Formats	Restrict the use of information inputs to [Assignment: organization-defined trusted sources] and/or [Assignment: organization-defined formats].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SI-10(06)	Information Input Validation | Injection Prevention	Prevent untrusted data injections.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SI-11	Error Handling	a. Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited; andb. Reveal error messages only to [Assignment: organization-defined personnel or roles].	Functional	Equal	Error Handling	TDA-19	Mechanisms exist to handle error conditions by: (1) Identifying potentially security-relevant error conditions; (2) Generating error messages that provide information necessary for corrective actions without revealing sensitive or potentially harmful information in error logs and administrative messages that could be exploited; and (3) Revealing error messages only to authorized personnel.	10		Moderate
SI-12	Information Management and Retention	Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines and operational requirements.	Functional	Intersects With	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	5		Low

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-53B Baseline
SI-12	Information Management and Retention	Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines and operational requirements.	Functional	Intersects With	Personal Data (PD) Retention & Disposal	PRI-05	Mechanisms exist to: (1) Retain Personal Data (PD), including metadata, for an organization-defined time period to fulfill the purpose(s) identified in the notice or as required by law; (2) Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of storage; and (3) Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived records).	5		Low
SI-12(01)	Information Management and Retention | Limit Personally Identifiable Information Elements	Limit personally identifiable information being processed in the information life cycle to the following elements of personally identifiable information: [Assignment: organization-defined elements of personally identifiable information].	Functional	Intersects With	Internal Use of Personal Data (PD) For Testing, Training and Research	PRI-05.1	Mechanisms exist to address the use of Personal Data (PD) for internal testing, training and research that: (1) Takes measures to limit or minimize the amount of PD used for internal testing, training and research purposes; and (2) Authorizes the use of PD when such information is required for internal testing, training and research.	5		Not Selected
SI-12(01)	Information Management and Retention | Limit Personally Identifiable Information Elements	Limit personally identifiable information being processed in the information life cycle to the following elements of personally identifiable information: [Assignment: organization-defined elements of personally identifiable information].	Functional	Intersects With	Minimize Sensitive / Regulated Data	DCH-18.1	Mechanisms exist to minimize sensitive/regulated data that is collected, received, processed, stored and/or transmitted throughout the information lifecycle to only those elements necessary to support necessary	5		Not Selected
SI-12(02)	Information Management and Retention | Minimize Personally Identifiable Information in Testing, Training, and Research	Use the following techniques to minimize the use of personally identifiable information for research, testing, or training: [Assignment: organization-defined techniques].	Functional	Intersects With	Limit Sensitive / Regulated Data In Testing, Training & Research	DCH-18.2	Mechanisms exist to minimize the use of sensitive/regulated data for research, testing, or training, in accordance with authorized, legitimate business practices.	5		Not Selected
SI-12(02)	Information Management and Retention | Minimize Personally Identifiable Information in Testing, Training, and Research	Use the following techniques to minimize the use of personally identifiable information for research, testing, or training: [Assignment: organization-defined techniques].	Functional	Intersects With	Internal Use of Personal Data (PD) For Testing, Training and Research	PRI-05.1	Mechanisms exist to address the use of Personal Data (PD) for internal testing, training and research that: (1) Takes measures to limit or minimize the amount of PD used for internal testing, training and research purposes; and (2) Authorizes the use of PD when such information is required for internal testing, training and research.	5		Not Selected
SI-12(03)	Information Management and Retention | Information Disposal	Use the following techniques to dispose of, destroy, or erase information following the retention period: [Assignment: organization-defined techniques].	Functional	Intersects With	Personal Data (PD) Retention & Disposal	PRI-05	Mechanisms exist to: (1) Retain Personal Data (PD), including metadata, for an organization-defined time period to fulfill the purpose(s) identified in the notice or as required by law; (2) Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of storage; and (3) Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived records).	5		Not Selected
SI-12(03)	Information Management and Retention | Information Disposal	Use the following techniques to dispose of, destroy, or erase information following the retention period: [Assignment: organization-defined techniques].	Functional	Intersects With	Information Disposal	DCH-21	Mechanisms exist to securely dispose of, destroy or erase information.	5		Not Selected
SI-13	Predictable Failure Prevention	a. Determine mean time to failure (MTTF) for the following system components in specific environments of operation: [Assignment: organization-defined system components]; andb. Provide substitute system components and a means to exchange active and standby components in accordance with the following criteria: [Assignment: organization-defined MTTF substitution criteria].	Functional	Intersects With	Failover Capability	BCD-12.2	Mechanisms exist to implement real-time or near-real-time failover capability to maintain availability of critical Technology Assets, Applications, Services and/or Data (TAASD).	5		Not Selected
SI-13	Predictable Failure Prevention	a. Determine mean time to failure (MTTF) for the following system components in specific environments of operation: [Assignment: organization-defined system components]; andb. Provide substitute system components and a means to exchange active and standby components in accordance with the following criteria: [Assignment: organization-defined MTTF substitution criteria].	Functional	Intersects With	Predictable Failure Analysis	SEA-07	Mechanisms exist to determine the Mean Time to Failure (MTTF) for system components in specific environments of operation.	5		Not Selected
SI-13(01)	Predictable Failure Prevention | Transferring Component Responsibilities	Take system components out of service by transferring component responsibilities to substitute components no later than [Assignment: organization-defined fraction or percentage] of mean time to failure.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SI-13(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Withdrawn
SI-13(03)	Predictable Failure Prevention | Manual Transfer Between Components	Manually initiate transfers between active and standby system components when the use of the active component reaches [Assignment: organization-defined percentage] of the mean time to failure.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SI-13(04)	Predictable Failure Prevention | Standby Component Installation and Notification	If system component failures are detected:a. Ensure that the standby components are successfully and transparently installed within [Assignment: organization-defined time period]; andb. [Selection (one or more): Activate [Assignment: organization-defined alarm]; Automatically shut down the system; [Assignment: organization-defined action]].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SI-13(05)	Predictable Failure Prevention | Failover Capability	Provide [Selection (one): real-time; near real-time] [Assignment: organization-defined failover capability] for the system.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SI-14	Non-persistence	Implement non-persistent [Assignment: organization-defined 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]].	Functional	Equal	Non-Persistence	SEA-08	Mechanisms exist to implement non-persistent system components and services that are initiated in a known state and terminated upon the end of the session of use or periodically at an organization-defined frequency.	10		Not Selected
SI-14(01)	Non-persistence | Refresh from Trusted Sources	Obtain software and data employed during system component and service refreshes from the following trusted sources: [Assignment: organization-defined trusted sources].	Functional	Equal	Refresh from Trusted Sources	SEA-08.1	Mechanisms exist to ensure that software and data needed for system component and service refreshes are obtained from trusted sources.	10		Not Selected
SI-14(02)	Non-persistence | Non-persistent Information	a. [Selection (one): Refresh [Assignment: organization-defined information] [Assignment: organization-defined frequency]; Generate [Assignment: organization-defined information] on demand]; andb. Delete information when no longer needed.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SI-14(03)	Non-persistence | Non-persistent Connectivity	Establish connections to the system on demand and terminate connections after [Selection (one): completion of a request; a period of non-use].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SI-15	Information Output Filtering	Validate information output from the following software programs and/or applications to ensure that the information is consistent with the expected content: [Assignment: organization-defined software programs and/or applications].	Functional	Equal	Information Output Filtering	SEA-09	Mechanisms exist to validate information output from software programs and/or applications to ensure that the information is consistent with the expected content.	10		Not Selected
SI-16	Memory Protection	Implement the following controls to protect the system memory from unauthorized code execution: [Assignment: organization-defined controls].	Functional	Equal	Memory Protection	SEA-10	Mechanisms exist to implement security safeguards to protect system memory from unauthorized code execution.	10		Moderate

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-53B Baseline
SI-17	Fail-safe Procedures	Implement the indicated fail-safe procedures when the indicated failures occur: [Assignment: organization-defined list of failure conditions and associated fail-safe procedures].	Functional	Equal	Fail Safe	SEA-07.3	Mechanisms exist to implement fail-safe procedures when failure conditions occur.	10		Not Selected
SI-18	Personally Identifiable Information Quality Operations	a. Check the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle [Assignment: organization-defined frequency]; andb. Correct or delete inaccurate or outdated personally identifiable information.	Functional	Intersects With	Data Quality Operations	DCH-22	Mechanisms exist to check for Redundant, Obsolete/Outdated, Toxic or Trivial (ROTT) data to ensure the accuracy, relevance, timeliness, impact, completeness and de-identification of information throughout the information lifecycle.	5		Not Selected
SI-18(01)	Personally Identifiable Information Quality Operations | Automation Support	Correct or delete personally identifiable information that is inaccurate or outdated, incorrectly determined regarding impact, or incorrectly de-identified using [Assignment: organization-defined automated mechanisms].	Functional	Intersects With	Data Quality Operations	DCH-22	Mechanisms exist to check for Redundant, Obsolete/Outdated, Toxic or Trivial (ROTT) data to ensure the accuracy, relevance, timeliness, impact, completeness and de-identification of information throughout the information lifecycle.	5		Not Selected
SI-18(02)	Personally Identifiable Information Quality Operations | Data Tags	Employ data tags to automate the correction or deletion of personally identifiable information across the information life cycle within organizational systems.	Functional	Equal	Data Tags	DCH-22.2	Mechanisms exist to utilize data tags to automate tracking of sensitive/regulated data across the information lifecycle.	10		Not Selected
SI-18(03)	Personally Identifiable Information Quality Operations |	Collect personally identifiable information directly from the individual.	Functional	Equal	Primary Source Personal Data (PD) Collection	DCH-22.3	Mechanisms exist to collect Personal Data (PD) directly from the individual.	10		Not Selected
SI-18(04)	Personally Identifiable Information Quality Operations | Individual Requests	Correct or delete personally identifiable information upon request by individuals or their designated representatives.	Functional	Intersects With	Correcting Inaccurate Personal Data (PD)	PRI-06.1	Mechanisms exist to maintain a process for: (1) Data subjects to have inaccurate Personal Data (PD) maintained by the organization corrected or amended; and (2) Disseminating corrections or amendments of PD to other authorized users of the PD.	5		Not Selected
SI-18(04)	Personally Identifiable Information Quality Operations | Individual Requests	Correct or delete personally identifiable information upon request by individuals or their designated representatives.	Functional	Intersects With	Updating & Correcting Personal Data (PD)	DCH-22.1	Mechanisms exist to utilize technical controls to correct Personal Data (PD) that is inaccurate or outdated, incorrectly determined regarding impact, or incorrectly de-identified.	5		Not Selected
SI-18(04)	Personally Identifiable Information Quality Operations | Individual Requests	Correct or delete personally identifiable information upon request by individuals or their designated representatives.	Functional	Intersects With	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request erasure of their PD; and (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	5		Not Selected
SI-18(05)	Personally Identifiable Information Quality Operations | Notice of Correction or Deletion	Notify [Assignment: organization-defined recipients of personally identifiable information] and individuals that the personally identifiable information has been corrected or deleted.	Functional	Intersects With	Updating & Correcting Personal Data (PD)	DCH-22.1	Mechanisms exist to utilize technical controls to correct Personal Data (PD) that is inaccurate or outdated, incorrectly determined regarding impact, or incorrectly de-identified.	5		Not Selected
SI-18(05)	Personally Identifiable Information Quality Operations | Notice of Correction or Deletion	Notify [Assignment: organization-defined recipients of personally identifiable information] and individuals that the personally identifiable information has been corrected or deleted.	Functional	Intersects With	Correcting Inaccurate Personal Data (PD)	PRI-06.1	Mechanisms exist to maintain a process for: (1) Data subjects to have inaccurate Personal Data (PD) maintained by the organization corrected or amended; and (2) Disseminating corrections or amendments of PD to other authorized users of the PD.	5		Not Selected
SI-18(05)	Personally Identifiable Information Quality Operations | Notice of Correction or Deletion	Notify [Assignment: organization-defined recipients of personally identifiable information] and individuals that the personally identifiable information has been corrected or deleted.	Functional	Intersects With	Notice of Correction or Processing Change	PRI-06.2	Mechanisms exist to notify affected data subjects if their Personal Data (PD) has been corrected, amended or deleted.	5		Not Selected
SI-19	De-identification	a. Remove the following elements of personally identifiable information from datasets: [Assignment: organization-defined elements of personally identifiable information]; andb. Evaluate [Assignment: organization-defined frequency] for effectiveness of de-identification.	Functional	Equal	De-Identification (Anonymization)	DCH-23	Mechanisms exist to anonymize data by removing Personal Data (PD) from datasets.	10		Not Selected
SI-19(01)	De-identification | Collection	De-identify the dataset upon collection by not collecting personally identifiable information.	Functional	Intersects With	Primary Source Personal Data (PD) Collection	DCH-22.3	Mechanisms exist to collect Personal Data (PD) directly from the individual.	5		Not Selected
SI-19(01)	De-identification | Collection	De-identify the dataset upon collection by not collecting personally identifiable information.	Functional	Intersects With	De-Identify Dataset Upon Collection	DCH-23.1	Mechanisms exist to de-identify the dataset upon collection by not collecting Personal Data (PD).	5		Not Selected
SI-19(02)	De-identification | Archiving	Prohibit archiving of personally identifiable information elements if those elements in a dataset will not be needed after the dataset is archived.	Functional	Equal	Archiving	DCH-23.2	Mechanisms exist to refrain from archiving Personal Data (PD) elements if those elements in a dataset will not be needed after the dataset is archived.	10		Not Selected
SI-19(03)	De-identification | Release	Remove personally identifiable information elements from a dataset prior to its release if those elements in the dataset do not need to be part of the data release.	Functional	Equal	Release	DCH-23.3	Mechanisms exist to remove Personal Data (PD) elements from a dataset prior to its release if those elements in the dataset do not need to be part of the data release.	10		Not Selected
SI-19(04)	De-identification | Removal, Masking, Encryption, Hashing, or Replacement of Direct Identifiers	Remove, mask, encrypt, hash, or replace direct identifiers in a dataset.	Functional	Intersects With	Data Masking	PRI-05.3	Mechanisms exist to mask sensitive/regulated data through data anonymization, pseudonymization, redaction or de-identification.	5		Not Selected
SI-19(04)	De-identification | Removal, Masking, Encryption, Hashing, or Replacement of Direct Identifiers	Remove, mask, encrypt, hash, or replace direct identifiers in a dataset.	Functional	Intersects With	Removal, Masking, Encryption, Hashing or Replacement of Direct Identifiers	DCH-23.4	Mechanisms exist to remove, mask, encrypt, hash or replace direct identifiers in a dataset.	5		Not Selected
SI-19(05)	De-identification | Statistical Disclosure Control	Manipulate numerical data, contingency tables, and statistical findings so that no individual or organization is identifiable in the results of the analysis.	Functional	Equal	Statistical Disclosure Control	DCH-23.5	Mechanisms exist to manipulate numerical data, contingency tables and statistical findings so that no person or organization is identifiable in the results of the analysis.	10		Not Selected
SI-19(06)	De-identification | Differential Privacy	Prevent disclosure of personally identifiable information by adding non-deterministic noise to the results of mathematical operations before the results are reported.	Functional	Equal	Differential Data Privacy	DCH-23.6	Mechanisms exist to prevent disclosure of Personal Data (PD) by adding non-deterministic noise to the results of mathematical operations before the results are reported.	10		Not Selected
SI-19(07)	De-identification | Validated Algorithms and Software	Perform de-identification using validated algorithms and software that is validated to implement the algorithms.	Functional	Equal	Automated De-Identification of Sensitive Data	DCH-23.7	Mechanisms exist to perform de-identification of sensitive/regulated data, using validated algorithms and software to implement the	10		Not Selected

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh	Notes	NIST SP 800-53B Baseline
SI-19(08)	De-identification | Motivated Intruder	Perform a motivated intruder test on the de-identified dataset to determine if the identified data remains or if the de-identified data can be re-identified.	Functional	Equal	Motivated Intruder	DCH-23.8	Mechanisms exist to perform a motivated intruder test on the de-identified dataset to determine if the identified data remains or if the de-identified data can be re-identified.	10		Not Selected
SI-20	Tainting	Embed data or capabilities in the following systems or system components to determine if organizational data has been exfiltrated or improperly removed from the organization: [Assignment: organization-defined systems or system components].	Functional	Equal	Tainting	THR-08	Mechanisms exist to embed false data or steganographic data in files to enable the organization to determine if data has been exfiltrated and provide a means to identify the individual(s) involved.	10		Not Selected
SI-21	Information Refresh	Refresh [Assignment: organization-defined information] at [Assignment: organization-defined frequencies] or generate the information on demand and delete the information when no longer needed.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SI-22	Information Diversity	a. Identify the following alternative sources of information for [Assignment: organization-defined essential functions and services]: [Assignment: organization-defined alternative information sources]; andb. Use an alternative information source for the execution of essential functions or services on [Assignment: organization-defined systems or system components] when the primary source of information is corrupted or unavailable.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SI-23	Information Fragmentation	Based on [Assignment: organization-defined circumstances]:a. Fragment the following information: [Assignment: organization-defined information]; andb. Distribute the fragmented information across the following systems or system components: [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SR-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] supply chain risk management policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the supply chain risk management policy and the associated supply chain risk management controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the supply chain risk management policy and procedures; andc. Review and update the current supply chain risk management:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5		Low
SR-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] supply chain risk management policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the supply chain risk management policy and the associated supply chain risk management controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the supply chain risk management policy and procedures; andc. Review and update the current supply chain risk management:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5		Low
SR-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] supply chain risk management policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the supply chain risk management policy and the associated supply chain risk management controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the supply chain risk management policy and procedures; andc. Review and update the current supply chain risk management:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10		Low
SR-02	Supply Chain Risk Management Plan	a. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the following systems, system components or system services: [Assignment: organization-defined systems, system components, or system services];b. Review and update the supply chain risk management plan [Assignment: organization-defined frequency] or as required, to address threat, organizational or environmental changes; andc. Protect the supply chain risk management plan from unauthorized disclosure and modification.	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5		Low
SR-02	Supply Chain Risk Management Plan	a. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the following systems, system components or system services: [Assignment: organization-defined systems, system components, or system services];b. Review and update the supply chain risk management plan [Assignment: organization-defined frequency] or as required, to address threat, organizational or environmental changes; andc. Protect the supply chain risk management plan from unauthorized disclosure and modification.	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and (2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	5		Low
SR-02(01)	Supply Chain Risk Management Plan | Establish SCRM Team	Establish a supply chain risk management team consisting of [Assignment: organization-defined personnel, roles, and responsibilities] to lead and support the following SCRM activities: [Assignment: organization-defined supply chain risk management activities].	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and (2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	5		Low

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh	Notes	NIST SP 800-53B Baseline
SR-03	Supply Chain Controls and Processes	a. Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of [Assignment: organization-defined system or system component] in coordination with [Assignment: organization-defined supply chain personnel];b. Employ the following controls to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain-related events: [Assignment: organization-defined supply chain controls]; andc. Document the selected and implemented supply chain processes and controls in [Selection (one): security and privacy plans; supply chain risk management plan; [Assignment: organization-defined document]].	Functional	Equal	Processes To Address Weaknesses or Deficiencies	TPM-03.3	Mechanisms exist to address identified weaknesses or deficiencies in the security of the supply chain	10		Low
SR-03(01)	Supply Chain Controls and Processes | Diverse Supply Base	Employ a diverse set of sources for the following system components and services: [Assignment: organization-defined system components and services].	Functional	Intersects With	Development Methods, Techniques & Processes	TDA-02.3	Mechanisms exist to require software developers to ensure that their software development processes employ industry-recognized secure practices for secure programming, engineering methods, quality control processes and validation techniques to minimize flawed and/or malformed software.	5		Not Selected
SR-03(01)	Supply Chain Controls and Processes | Diverse Supply Base	Employ a diverse set of sources for the following system components and services: [Assignment: organization-defined system components and services].	Functional	Intersects With	Supplier Diversity	TDA-03.1	Mechanisms exist to obtain security, compliance and resilience technologies from different suppliers to minimize supply chain risk.	5		Not Selected
SR-03(01)	Supply Chain Controls and Processes | Diverse Supply Base	Employ a diverse set of sources for the following system components and services: [Assignment: organization-defined system components and services].	Functional	Intersects With	Acquisition Strategies, Tools & Methods	TPM-03.1	Mechanisms exist to utilize tailored acquisition strategies, contract tools and procurement methods for the purchase of unique Technology Assets, Applications and/or Services.	5		Not Selected
SR-03(02)	Supply Chain Controls and Processes | Limitation of Harm	Employ the following controls to limit harm from potential adversaries identifying and targeting the organizational supply chain: [Assignment: organization-defined controls].	Functional	Equal	Limit Potential Harm	TPM-03.2	Mechanisms exist to utilize security safeguards to limit harm from potential adversaries who identify and target the organization's supply chain.	10		Not Selected
SR-03(03)	Supply Chain Controls and Processes | Sub-tier Flow Down	Ensure that the controls included in the contracts of prime contractors are also included in the contracts of subcontractors.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5		Not Selected
SR-03(03)	Supply Chain Controls and Processes | Sub-tier Flow Down	Ensure that the controls included in the contracts of prime contractors are also included in the contracts of subcontractors.	Functional	Intersects With	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	5		Not Selected
SR-04	Provenance	Document, monitor, and maintain valid provenance of the following systems, system components, and associated data: [Assignment: organization-defined systems, system components, and associated data].	Functional	Intersects With	Provenance	AST-03.2	Mechanisms exist to track the origin, development, ownership, location and changes to Technology Assets, Applications, Services and/or Data (TAASD).	5		Not Selected
SR-04(01)	Provenance | Identity	Establish and maintain unique identification of the following supply chain elements, processes, and personnel associated with the identified system and critical system components: [Assignment: organization-defined supply chain elements, processes, and personnel associated with organization-defined systems and critical system components].	Functional	Intersects With	Provenance	AST-03.2	Mechanisms exist to track the origin, development, ownership, location and changes to Technology Assets, Applications, Services and/or Data (TAASD).	5		Not Selected
SR-04(02)	Provenance | Track and Trace	Establish and maintain unique identification of the following systems and critical system components for tracking through the supply chain: [Assignment: organization-defined systems and critical system components].	Functional	Intersects With	Provenance	AST-03.2	Mechanisms exist to track the origin, development, ownership, location and changes to Technology Assets, Applications, Services and/or Data (TAASD).	5		Not Selected
SR-04(03)	Provenance | Validate as Genuine and Not Altered	Employ the following controls to validate that the system or system component received is genuine and has not been altered: [Assignment: organization-defined controls].	Functional	Intersects With	Product Tampering and Counterfeiting (PTC)	TDA-11	Mechanisms exist to maintain awareness of component authenticity by developing and implementing Product Tampering and Counterfeiting (PTC) practices that include the means to detect and prevent counterfeit components.	5		Not Selected
SR-04(04)	Provenance | Supply Chain Integrity — Pedigree	Employ [Assignment: organization-defined controls] and conduct [Assignment: organization-defined analysis] to ensure the integrity of the system and system components by validating the internal composition and provenance of critical or mission-essential technologies, products, and services.	Functional	Intersects With	Product Tampering and Counterfeiting (PTC)	TDA-11	Mechanisms exist to maintain awareness of component authenticity by developing and implementing Product Tampering and Counterfeiting (PTC) practices that include the means to detect and prevent counterfeit components.	5		Not Selected
SR-05	Acquisition Strategies, Tools, and Methods	Employ the following acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks: [Assignment: organization-defined acquisition strategies, contract tools, and procurement methods].	Functional	Intersects With	Acquisition Strategies, Tools & Methods	TPM-03.1	Mechanisms exist to utilize tailored acquisition strategies, contract tools and procurement methods for the purchase of unique Technology Assets, Applications and/or Services.	5		Low
SR-05(01)	Acquisition Strategies, Tools, and Methods | Adequate Supply	Employ the following controls to ensure an adequate supply of [Assignment: organization-defined critical system components]: [Assignment: organization-defined controls].	Functional	Equal	Adequate Supply	TPM-03.4	Mechanisms exist to develop and implement a spare parts strategy to ensure that an adequate supply of critical components is available to meet operational needs.	10		Not Selected
SR-05(02)	Strategies, Tools, and Methods | Assessments Prior to Selection, Acceptance, Modification, or	Assess the system, system component, or system service prior to selection, acceptance, modification, or update.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	Not Selected
SR-06	Supplier Assessments and Reviews	Assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide [Assignment: organization-defined frequency].	Functional	Intersects With	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5		Moderate
SR-06(01)	Supplier Assessments and Reviews | Testing and Analysis	Employ [Selection (one or more): organizational analysis; independent third-party analysis; organizational testing; independent third-party testing] of the following supply chain elements, processes, and actors associated with the system, system component, or system service: [Assignment: organization-defined supply chain elements, processes, and actors].	Functional	Intersects With	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5		Not Selected
SR-07	Supply Chain Operations Security	Employ the following Operations Security (OPSEC) controls to protect supply chain-related information for the system, system component, or system service: [Assignment: organization-defined Operations Security (OPSEC) controls].	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5		Not Selected
SR-07	Supply Chain Operations Security	Employ the following Operations Security (OPSEC) controls to protect supply chain-related information for the system, system component, or system service: [Assignment: organization-defined Operations Security (OPSEC) controls].	Functional	Intersects With	Operations Security	OPS-01	Mechanisms exist to facilitate the implementation of operational security controls.	5		Not Selected
SR-08	Notification Agreements	Establish agreements and procedures with entities involved in the supply chain for the system, system component, or system service for the [Selection (one or more): notification of supply chain compromises; results of assessments or audits; [Assignment: organization-defined information]].	Functional	Equal	Security Compromise Notification Agreements	TPM-05.1	Mechanisms exist to compel External Service Providers (ESPs) to provide notification of actual or potential compromises in the supply chain that can potentially affect or have adversely affected Technology Assets, Applications and/or Services (TAAS) that the organization utilizes.	10		Low

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh	Notes	NIST SP 800-53B Baseline
SR-09	Tamper Resistance and Detection	Implement a tamper protection program for the system, system component, or system service.	Functional	Intersects With	Logical Tampering Protection	AST-15	Mechanisms exist to assess the integrity of critical Technology Assets, Applications and/or Services (TAAS) to detect evidence of tampering, where: (1) Logical assessments evaluate the integrity of critical components (e.g., configuration settings); and (2) Physical assessments evaluate assets for evidence of unauthorized access and/or	5		High
SR-09(01)	Tamper Resistance and Detection | Multiple Stages of System Development Life Cycle	Employ anti-tamper technologies, tools, and techniques throughout the system development life cycle.	Functional	Intersects With	Logical Tampering Protection	AST-15	Mechanisms exist to assess the integrity of critical Technology Assets, Applications and/or Services (TAAS) to detect evidence of tampering, where: (1) Logical assessments evaluate the integrity of critical components (e.g., configuration settings); and (2) Physical assessments evaluate assets for evidence of unauthorized access and/or	5		High
SR-10	Inspection of Systems or Components	Inspect the following systems or system components [Selection (one or more): at random; at [Assignment: organization-defined frequency], upon [Assignment: organization-defined indications of need for inspection]] to detect tampering: [Assignment: organization-defined systems or system components].	Functional	Intersects With	Product Tampering and Counterfeiting (PTC)	TDA-11	Mechanisms exist to maintain awareness of component authenticity by developing and implementing Product Tampering and Counterfeiting (PTC) practices that include the means to detect and prevent counterfeit components.	5		Low
SR-10	Inspection of Systems or Components	Inspect the following systems or system components [Selection (one or more): at random; at [Assignment: organization-defined frequency], upon [Assignment: organization-defined indications of need for inspection]] to detect tampering: [Assignment: organization-defined systems or system components].	Functional	Intersects With	Technology Asset Inspections	AST-15.1	Mechanisms exist to physically and logically inspect critical technology assets to detect evidence of tampering.	5		Low
SR-11	Component Authenticity	a. Develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system; andb. Report counterfeit system components to [Selection (one or more): source of counterfeit component; [Assignment: organization-defined external reporting organizations]; [Assignment: organization-defined personnel or roles]].	Functional	Intersects With	Product Tampering and Counterfeiting (PTC)	TDA-11	Mechanisms exist to maintain awareness of component authenticity by developing and implementing Product Tampering and Counterfeiting (PTC) practices that include the means to detect and prevent counterfeit components.	5		Low
SR-11(01)	Component Authenticity | Anti-counterfeit Training	Train [Assignment: organization-defined personnel or roles] to detect counterfeit system components (including hardware, software, and firmware).	Functional	Equal	Anti-Counterfeit Training	TDA-11.1	Mechanisms exist to train personnel to detect counterfeit system components, including hardware, software and firmware.	10		Low
SR-11(02)	Component Authenticity | Configuration Control for Component Service and Repair	Maintain configuration control over the following system components awaiting service or repair and serviced or repaired components awaiting return to service: [Assignment: organization-defined system components].	Functional	Equal	Maintain Configuration Control During Maintenance	MNT-07	Mechanisms exist to maintain proper physical security and configuration control over technology assets awaiting service or repair.	10		Low
SR-11(03)	Component Authenticity | Anti-counterfeit Scanning	Scan for counterfeit system components [Assignment: organization-defined frequency].	Functional	Intersects With	Product Tampering and Counterfeiting (PTC)	TDA-11	Mechanisms exist to maintain awareness of component authenticity by developing and implementing Product Tampering and Counterfeiting (PTC) practices that include the means to detect and prevent counterfeit components.	5		Not Selected
SR-12	Component Disposal	Dispose of [Assignment: organization-defined data, documentation, tools, or system components] using the following techniques and methods: [Assignment: organization-defined techniques and methods].	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5		Low

Family	Sorting Control #	Focal Document Element	Focal Document Element Name	Focal Document Element Description	NIST SP 800-53 R5.2	Security Control Baseline	Set Theory Relationship Mapping (STRM) Rationale	Set Theory Relationship Mapping (STRM) Relationship	Set Theory Relationship Mapping (STRM) Strength of Relationship	Reference Document Element	Reference Document Element Name	Reference Document Element Description	NIST SP 800-53 R5.2 Baselines Low	Mod	High	Privacy	FedRAMP R5 Low	Mod	High	LI-SaaS	NIST SP 800-161 R1 C-SCRM Baseline	Low-Impact Software Development	Level 1	Level 2	Level 3	GovRAMP Low	Low+	Moderate	Core	High (FedRAMP Hi
AC	AC-01	AC-1	Policy and Procedures	[Assignment: organization-defined personnel or roles] is/are to be made aware of the policies, standards, and procedures established by the organization's information security program.	AC-1	Low	Functional	Intersects With	5	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	AC-1	AC-1	AC-1	AC-1	AC-01	AC-01	AC-01	AC-01	AC-1	AC-1	AC-1	AC-1	AC-1	AC-01	AC-01	AC-01		AC-01
AC	AC-01	AC-1	Policy and Procedures	[Assignment: organization-defined personnel or roles] is/are to be made aware of the policies, standards, and procedures established by the organization's information security program.	AC-1	Low	Functional	Intersects With	5	Cybersecurity & Data Protection Governance Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	AC-1	AC-1	AC-1	AC-1	AC-01	AC-01	AC-01	AC-01	AC-1	AC-1	AC-1	AC-1	AC-1	AC-01	AC-01	AC-01		AC-01
AC	AC-01	AC-1	Policy and Procedures	[Assignment: organization-defined personnel or roles] is/are to be made aware of the policies, standards, and procedures established by the organization's information security program.	AC-1	Low	Functional	Subset Of	10	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	AC-1	AC-1	AC-1	AC-1	AC-01	AC-01	AC-01	AC-01	AC-1	AC-1	AC-1	AC-1	AC-1	AC-01	AC-01	AC-01		AC-01
AC	AC-02	AC-2	Account Management	[Assignment: organization-defined personnel or roles] is/are to be made aware of the policies, standards, and procedures established by the organization's information security program.	AC-2	Low	Functional	Intersects With	5	Termination of Employment	IAC-07.2	Mechanisms exist to revoke user access rights in a timely manner, upon termination of employment or contract.	AC-2	AC-2	AC-2	AC-2	AC-02	AC-02	AC-02	AC-02	AC-2	AC-2	AC-2	AC-2	AC-2	AC-02	AC-02	AC-02	AC-02	AC-02
AC	AC-02	AC-2	Account Management	[Assignment: organization-defined personnel or roles] is/are to be made aware of the policies, standards, and procedures established by the organization's information security program.	AC-2	Low	Functional	Intersects With	5	Account Management	IAC-15	Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.	AC-2	AC-2	AC-2	AC-2	AC-02	AC-02	AC-02	AC-02	AC-2	AC-2	AC-2	AC-2	AC-2	AC-02	AC-02	AC-02	AC-02	AC-02
AC	AC-02	AC-2	Account Management	[Assignment: organization-defined personnel or roles] is/are to be made aware of the policies, standards, and procedures established by the organization's information security program.	AC-2	Low	Functional	Intersects With	5	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	AC-2	AC-2	AC-2	AC-2	AC-02	AC-02	AC-02	AC-02	AC-2	AC-2	AC-2	AC-2	AC-2	AC-02	AC-02	AC-02	AC-02	AC-02
AC	AC-02	AC-2	Account Management	[Assignment: organization-defined personnel or roles] is/are to be made aware of the policies, standards, and procedures established by the organization's information security program.	AC-2	Low	Functional	Intersects With	5	Safeguarding Data Over Open Networks	NET-12	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.	AC-2	AC-2	AC-2	AC-2	AC-02	AC-02	AC-02	AC-02	AC-2	AC-2	AC-2	AC-2	AC-2	AC-02	AC-02	AC-02	AC-02	AC-02
AC	AC-02(01)	AC-2(1)	Account Management | Automated System Account Management	[Assignment: organization-defined automated mechanisms] to support the management of system accounts.	AC-2(1)	Moderate	Functional	Intersects With	5	Automated System Account Management (Directory Services)	IAC-15.1	Automated mechanisms exist to support the management of system accounts (e.g., directory services).		AC-2(1)	AC-2(1)			AC-02(01)	AC-02(01)									AC-02(01)	AC-02(01)	AC-02(01)	AC-02(01)
AC	AC-02(02)	AC-2(2)	Account Management | Automated Temporary and Emergency Account Management	[Assignment: organization-defined automated mechanisms] to [Assignment: organization-defined time period] for each type of account.	AC-2(2)	Moderate	Functional	Equal	10	Removal of Temporary / Emergency Accounts	IAC-15.2	Automated mechanisms exist to disable or remove temporary and emergency accounts after an organization-defined time period for each type of account.		AC-2(2)	AC-2(2)			AC-02(02)	AC-02(02)									AC-2(2)		AC-2(2)	
AC	AC-02(03)	AC-2(3)	Account Management | Disable Accounts	[Assignment: organization-defined time period] when accounts: (a) Have expired; (b) Are no longer associated with a user or individual; (c) Are in violation of organizational policy; and (d) Have been inactive for [Assignment: organization-defined time period].	AC-2(3)	Moderate	Functional	Equal	10	Disable Inactive Accounts	IAC-15.3	Automated mechanisms exist to disable inactive accounts after an organization-defined time period.		AC-2(3)	AC-2(3)			AC-02(03)	AC-02(03)									AC-2(3)		AC-2(3)	
AC	AC-02(04)	AC-2(4)	Account Management | Automated Audit Actions	[Assignment: organization-defined automated mechanisms] to [Assignment: organization-defined actions] for [Assignment: organization-defined accounts].	AC-2(4)	Moderate	Functional	Equal	10	Automated Audit Actions	IAC-15.4	Automated mechanisms exist to audit account creation, modification, enabling, disabling and removal actions and notify [Assignment: organization-defined personnel or roles].		AC-2(4)	AC-2(4)			AC-02(04)	AC-02(04)									AC-2(4)		AC-2(4)	
AC	AC-02(05)	AC-2(5)	Account Management | Inactivity Logout	[Assignment: organization-defined time period of expected inactivity] or [Assignment: organization-defined circumstances].	AC-2(5)	Moderate	Functional	Equal	10	Session Lock	IAC-24	Mechanisms exist to initiate a session lock after an organization-defined time period of inactivity, or upon receiving a request from a user and retain the session lock until the user reestablishes access using established identification and authentication methods.		AC-2(5)	AC-2(5)			AC-02(05)	AC-02(05)									AC-2(5)		AC-2(5)	
AC	AC-02(06)	AC-2(6)	Account Management | Dynamic Privilege Management	[Assignment: organization-defined dynamic privilege management capabilities].	AC-2(6)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
AC	AC-02(07)	AC-2(7)	Account Management | Privileged User Accounts	[Assignment: organization-defined privileged roles] are organized into [Assignment: organization-defined accounts]; Monitor privileged role or attribute assignments; Monitor changes to roles or attributes; and Revoke access when [Assignment: organization-defined conditions].	AC-2(7)	Not Selected	Functional	Equal	10	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.						AC-02(07)	AC-02(07)									AC-02(07)	AC-02(07)	AC-02(07)	AC-02(07)
AC	AC-02(08)	AC-2(8)	Account Management | Dynamic Account Management	Create, activate, manage, and deactivate [Assignment: organization-defined system accounts] dynamically.	AC-2(8)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
AC	AC-02(09)	AC-2(9)	Account Management | Restrictions on Use of Shared and Group Accounts	Only permit the use of shared and group accounts that meet [Assignment: organization-defined conditions for establishing shared and group accounts].	AC-2(9)	Not Selected	Functional	Equal	10	Restrictions on Shared Groups / Accounts	IAC-15.5	Mechanisms exist to authorize the use of shared/group accounts only under certain organization-defined conditions.						AC-02(09)	AC-02(09)									AC-2(9)		AC-2(9)	
AC	AC-02(10)	AC-2(10)		Withdrawn	AC-2(10)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																	AC-2(10)		AC-2(10)	
AC	AC-02(11)	AC-2(11)	Account Management | Usage Conditions	Enforce [Assignment: organization-defined circumstances and/or usage conditions] for [Assignment: organization-defined accounts].	AC-2(11)	High	Functional	Equal	10	Usage Conditions	IAC-15.8	Automated mechanisms exist to enforce usage conditions for users and/or roles.			AC-2(11)				AC-02(11)											AC-2(11)	
AC	AC-02(12)	AC-2(12)	Account Management | Account Monitoring for Atypical Usage	Monitor system accounts for [Assignment: organization-defined atypical usage]; and Report atypical usage of system accounts to [Assignment: organization-defined personnel or roles].	AC-2(12)	High	Functional	Equal	10	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.			AC-2(12)	AC-2(12)			AC-02(12)										AC-2(12)		AC-2(12)	
AC	AC-02(13)	AC-2(13)	Account Management | Disable Accounts for High-risk Individuals	Disable accounts of high-risk individuals within [Assignment: organization-defined time period] of discovery of [Assignment: organization-defined significant risks].	AC-2(13)	Moderate	Functional	Intersects With	5	High-Risk Terminations	HRS-09.2	Mechanisms exist to expedite the process of removing "high risk" individual's access to Technology Assets, Applications, Services and/or Data (TAASD) upon termination, as determined by management.	AC-2(13)	AC-2(13)	AC-2(13)	AC-2(13)	AC-02(13)	AC-02(13)	AC-02(13)	AC-02(13)	AC-2(13)	AC-2(13)	AC-2(13)	AC-2(13)	AC-2(13)					AC-2(13)
AC	AC-02(13)	AC-2(13)	Account Management | Disable Accounts for High-risk Individuals	Disable accounts of high-risk individuals within [Assignment: organization-defined time period] of discovery of [Assignment: organization-defined significant risks].	AC-2(13)	Moderate	Functional	Intersects With	5	Account Disabling for High Risk Individuals	IAC-15.6	Mechanisms exist to disable accounts immediately upon notification for users posing a significant risk to the organization.	AC-2(13)	AC-2(13)	AC-2(13)	AC-2(13)	AC-02(13)	AC-02(13)	AC-02(13)	AC-02(13)	AC-2(13)	AC-2(13)	AC-2(13)	AC-2(13)	AC-2(13)					AC-2(13)
AC	AC-03	AC-3	Access Enforcement	Enforce approved authorizations for logical access to information and system resources in accordance with [Assignment: organization-defined access control policy].	AC-3	Low	Functional	Intersects With	5	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	AC-3	AC-3	AC-3	AC-3	AC-03	AC-03	AC-03	AC-03	AC-3	AC-3	AC-3	AC-3	AC-3	AC-03	AC-03	AC-03		AC-03
AC	AC-03	AC-3	Access Enforcement	Enforce approved authorizations for logical access to information and system resources in accordance with [Assignment: organization-defined access control policy].	AC-3	Low	Functional	Intersects With	5	Safeguarding Data Over Open Networks	NET-12	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.	AC-3	AC-3	AC-3	AC-3	AC-03	AC-03	AC-03	AC-03	AC-3	AC-3	AC-3	AC-3	AC-3	AC-03	AC-03	AC-03		AC-03
AC	AC-03	AC-3	Access Enforcement	Enforce approved authorizations for logical access to information and system resources in accordance with [Assignment: organization-defined access control policy].	AC-3	Low	Functional	Intersects With	5	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	AC-3	AC-3	AC-3	AC-3	AC-03	AC-03	AC-03	AC-03	AC-3	AC-3	AC-3	AC-3	AC-3	AC-03	AC-03	AC-03		AC-03
AC	AC-03(01)	AC-3(1)		Withdrawn	AC-3(1)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
AC	AC-03(02)	AC-3(2)	Access Enforcement | Dual Authorization	Enforce dual authorization for [Assignment: organization-defined privileged commands and/or other organization-defined privileged commands and/or other organization-defined actions].	AC-3(2)	Not Selected	Functional	Intersects With	5	Two-Person Rule	HRS-12.1	Mechanisms exist to enforce a two-person rule for implementing changes to sensitive Technology Assets, Applications and/or Services (TAAS).	AC-3(2)	AC-3(2)	AC-3(2)	AC-3(2)	AC-03(02)	AC-03(02)	AC-03(02)	AC-03(02)	AC-3(2)	AC-3(2)	AC-3(2)	AC-3(2)	AC-3(2)					
AC	AC-03(02)	AC-3(2)	Access Enforcement | Dual Authorization	Enforce dual authorization for [Assignment: organization-defined privileged commands and/or other organization-defined privileged commands and/or other organization-defined actions].	AC-3(2)	Not Selected	Functional	Equal	10	Dual Authorization for Privileged Commands	IAC-20.5	Automated mechanisms exist to enforce dual authorization for privileged commands.	AC-3(2)	AC-3(2)	AC-3(2)	AC-3(2)	AC-03(02)	AC-03(02)	AC-03(02)	AC-03(02)	AC-3(2)	AC-3(2)	AC-3(2)	AC-3(2)	AC-3(2)					
AC	AC-03(03)	AC-3(3)	Access Enforcement | Mandatory Access Control	Enforce [Assignment: organization-defined mandatory access control policy] over all subjects and objects where the policy specifies that a subject that has been granted access to information is constrained from doing any of the following; Pass the information to any other subjects or objects; Grant its privileges to other subjects; Change one or more security attributes (specified by the policy) on subjects, objects, the system, or system components; Choose the security attributes to be associated with newly created or modified objects; and Change the rules governing access control.	AC-3(3)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
AC	AC-03(04)	AC-3(4)	Access Enforcement | Discretionary Access Control	Enforce [Assignment: organization-defined discretionary access control policy] over defined subjects and objects where the policy specifies that a subject that has been granted access to information is constrained from doing any of the following; Pass the information to any other subjects or objects; Grant its privileges to other subjects; Change security attributes on subjects, objects, the system or system components; Choose the security attributes to be associated with newly created or revised objects; or Change the rules governing access control.	AC-3(4)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
AC	AC-03(05)	AC-3(5)	Access Enforcement | Security-relevant Information	Enforce the following additional [Assignment: organization-defined mandatory access control policies] over the set of covered subjects and objects specified in the policy, and where the policy specifies that a subject that has been granted access to [Assignment: organization-defined security-relevant information] is constrained from doing any of the following; Pass the information to any other subjects or objects; Grant its privileges to other subjects; Change security attributes on subjects, objects, the system or system components; Choose the security attributes to be associated with newly created or modified objects; or Change the rules governing access control.	AC-3(5)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
AC	AC-03(06)	AC-3(6)		Withdrawn	AC-3(6)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
AC	AC-03(07)	AC-3(7)	Access Enforcement | Role-based Access Control	Enforce a role-based access control policy over defined subjects and objects and control access based upon [Assignment: organization-defined roles and users authorized to assume such roles].	AC-3(7)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
AC	AC-03(08)	AC-3(8)	Access Enforcement | Revocation of Access Authorizations	Enforce the revocation of access authorizations resulting from changes to the security attributes of subjects and objects based on [Assignment: organization-defined rules governing the timing of revocations of access authorizations].	AC-3(8)	Not Selected	Functional	Equal	10	Revocation of Access Authorizations	IAC-20.6	Mechanisms exist to revoke logical and physical access authorizations.												AC-3(8)	AC-3(8)					
AC	AC-03(09)	AC-3(9)	Access Enforcement | Controlled Release	Release information outside of the system only if; The receiving [Assignment: organization-defined systems or system components] provide [Assignment: organization-defined controls]; and; [Assignment: organization-defined organizational personnel or roles] authorize the release of information; and Using [Assignment: organization-defined mechanisms], the information is encrypted before release.	AC-3(9)	Not Selected	Functional	Equal	10	Controlled Release	DCH-03.3	Automated mechanisms exist to validate cybersecurity and data protection attributes prior to releasing information to external Technology Assets, Applications and/or Services (TAAS).												AC-3(9)	AC-3(9)					
AC	AC-03(10)	AC-3(10)	Access Enforcement | Audited Override of Access Control Mechanisms	Employ an audited override of automated access control mechanisms under [Assignment: organization-defined conditions]; and Audit the execution of the override in [Assignment: organization-defined auditable events].	AC-3(10)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
AC	AC-03(11)	AC-3(11)	Access Enforcement | Restrict Access to Specific Information Types	Restrict access to data repositories containing [Assignment: organization-defined information types].	AC-3(11)	Not Selected	Functional	Equal	10	Sensitive / Regulated Data Access Enforcement	CFG-08	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to restrict access to sensitive/regulated data.																		
AC	AC-03(12)	AC-3(12)	Access Enforcement | Assert and Enforce Application Access	Require applications to assert, as part of the installation process, the purposes for which the application is configured to access specific information and data; and Enforce the assertions.	AC-3(12)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
AC	AC-03(13)	AC-3(13)	Access Enforcement | Attribute-based Access Control	Enforce attribute-based access control policy over defined subjects and objects and control access based upon [Assignment: organization-defined attributes to assume access permissions].	AC-3(13)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
AC	AC-03(14)	AC-3(14)	Access Enforcement | Individual Access	Provide mechanisms to enable individuals to have access to the following elements of their personally identifiable information: [Assignment: organization-defined elements].	AC-3(14)	Not Selected	Functional	Equal	10	Data Subject Empowerment	PRI-06	(1) Receive a copy of their PD, in a structured, commonly used and machine-readable format that includes all PD that is transmitted, shared, updated and/or disposed; (2) Request corrections to their PD that is transmitted, shared, updated and/or disposed; (3) Obtain the source(s) of their PD;					AC-3(14)													
AC	AC-03(15)	AC-3(15)	Access Enforcement | Discretionary and Mandatory Access Control	Enforce [Assignment: organization-defined mandatory access control policy] over the set of covered subjects and objects specified in the policy; and; Enforce [Assignment: organization-defined discretionary access control policy] over the set of covered subjects and objects specified in the policy.	AC-3(15)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
AC	AC-04	AC-4	Information Flow Enforcement	Enforce approved authorizations for controlling the flow of information within the system and between connected systems based on [Assignment: organization-defined information flow control policies].	AC-4	Moderate	Functional	Equal	10	Data Flow Enforcement – Access Control Lists (ACLs)	NET-04	Mechanisms exist to design, implement and review firewall and router configurations to restrict connections between untrusted networks and internal systems.		AC-4	AC-4			AC-04	AC-04			AC-4		AC-4	AC-4		AC-04	AC-04	AC-04	AC-04	AC-04
AC	AC-04(01)	AC-4(1)	Information Flow Enforcement | Object Security and Privacy Attributes	Use [Assignment: organization-defined information, source, and destination objects] to enforce [Assignment: organization-defined information flow control policies].	AC-4(1)	Not Selected	Functional	Equal	10	Object Security Attributes	NET-04.2	Mechanisms exist to associate security attributes with information, source and destination objects to enforce defined information flow control configurations as a basis for flow control decisions.																		
AC	AC-04(02)	AC-4(2)	Information Flow Enforcement | Processing Domains	Use protected processing domains to enforce [Assignment: organization-defined information flow control policies].	AC-4(2)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
AC	AC-04(03)	AC-4(3)	Information Flow Enforcement | Dynamic Information Flow Control	Enforce [Assignment: organization-defined information flow control policies].	AC-4(3)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
AC	AC-04(04)	AC-4(4)	Information Flow Enforcement | Flow Control of Encrypted Information	Prevent [Assignment: organization-defined encrypted information]; terminating communications sessions attempting to send encrypted information that is not authorized; and Enforcing [Assignment: organization-defined limitations].	AC-4(4)	High	Functional	Equal	10	Content Check for Encrypted Data	NET-04.3	Mechanisms exist to prevent encrypted data from bypassing content-checking mechanisms.			AC-4(4)				AC-04(04)												
AC	AC-04(05)	AC-4(5)	Information Flow Enforcement | Embedded Data Types	Enforce [Assignment: organization-defined limitations] on embedding data types within other data types.	AC-4(5)	Not Selected	Functional	Equal	10	Embedded Data Types	NET-04.4	Mechanisms exist to enforce limitations on embedding data within other data types.																		
AC	AC-04(06)	AC-4(6)	Information Flow Enforcement | Metadata	Enforce information flow control based on [Assignment: organization-defined metadata].	AC-4(6)	Not Selected	Functional	Equal	10	Metadata	NET-04.5	Mechanisms exist to enforce information flow controls based on metadata.												AC-4(6)	AC-4(6)					
AC	AC-04(07)	AC-4(7)	Information Flow Enforcement | One-way Flow Mechanisms	Enforce one-way information flows through hardware-based flow control mechanisms.	AC-4(7)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
AC	AC-04(08)	AC-4(8)	Information Flow Enforcement | Security and Privacy Policy Filters	Enforce the following security or privacy policy filters when data structures are passed between [Assignment: organization-defined information flows]: [Selection (one or more): Block; Strip; Modify; Quarantine] data that is inconsistent with [Assignment: organization-defined security or privacy policy filters].	AC-4(8)	Not Selected	Functional	Equal	10	Policy Decision Point (PDP)	NET-04.7	Automated mechanisms exist to evaluate access requests against established criteria to dynamically and uniformly enforce access rights and permissions.																		AC-04(08)
AC	AC-04(09)	AC-4(9)	Information Flow Enforcement | Human Reviews	Enforce the following security or privacy policy filters when data structures are passed between [Assignment: organization-defined information flows]: [Assignment: organization-defined security or privacy policy filters] under the following conditions: [Assignment: organization-defined conditions].	AC-4(9)	Not Selected	Functional	Equal	10	Human Reviews	NET-04.6	Mechanisms exist to enforce the use of human reviews for Access Control Lists (ACLs) and similar rulesets on a routine basis.																		
AC	AC-04(10)	AC-4(10)	Information Flow Enforcement | Enable and Disable Security or Privacy Policy Filters	Provide the capability for privileged administrators to enable and disable [Assignment: organization-defined security or privacy policy filters] under the following conditions: [Assignment: organization-defined conditions].	AC-4(10)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
AC	AC-04(11)	AC-4(11)	Information Flow Enforcement | Configuration of Security or Privacy Policy Filters	Provide the capability for privileged administrators to configure [Assignment: organization-defined security or privacy policy filters] to support different security or privacy characteristics for different [Assignment: organization-defined information flows].	AC-4(11)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
AC	AC-04(12)	AC-4(12)	Information Flow Enforcement | Data Type Identifiers	When transferring information between different security domains, use [Assignment: organization-defined data type identifiers] to validate data essential for information flow decisions.	AC-4(12)	Not Selected	Functional	Equal	10	Data Type Identifiers	NET-04.8	Automated mechanisms exist to utilize data type identifiers to validate data essential for information flow decisions when transferring information between different security domains.																		
AC	AC-04(13)	AC-4(13)	Information Flow Enforcement | Decomposition into Policy-relevant Subcomponents	When transferring information between different security domains, decompose information into [Assignment: organization-defined policy-relevant subcomponents] for submission to policy enforcement mechanisms.	AC-4(13)	Not Selected	Functional	Equal	10	Decomposition into Policy-Related Subcomponents	NET-04.9	Automated mechanisms exist to enforce information flow control by decomposing information into policy-relevant subcomponents for submission to policy enforcement mechanisms, when transferring information between different security domains.																		
AC	AC-04(14)	AC-4(14)	Information Flow Enforcement | Security or Privacy Policy Filter Constraints	Enforce the following security or privacy policy filters when data structures are passed between different security domains: [Assignment: organization-defined security or privacy policy filters] requiring fully enumerated formats that restrict data structure and content.	AC-4(14)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
AC	AC-04(15)	AC-4(15)	Information Flow Enforcement | Detection of Unsanctioned Information	When transferring information between different security domains, examine the information for the presence of [Assignment: organization-defined unsanctioned information] and prohibit the transfer of such information in accordance with [Assignment: organization-defined security policy].	AC-4(15)	Not Selected	Functional	Equal	10	Detection of Unsanctioned Information	NET-04.10	Automated mechanisms exist to examine information for the presence of unsanctioned information and prohibits the transfer of such information, when transferring information between different security domains.																		
AC	AC-04(16)	AC-4(16)		Withdrawn	AC-4(16)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
AC	AC-04(17)	AC-4(17)	Information Flow Enforcement | Domain Authentication	Uniquely identify and authenticate source and destination points for [Selection (one or more): organization; system; application; service; individual] for information transfer.	AC-4(17)	Not Selected	Functional	Equal	10	Cross Domain Authentication	NET-04.12	Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.											AC-4(17)	AC-4(17)						
AC	AC-04(18)	AC-4(18)		Withdrawn	AC-4(18)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
AC	AC-04(19)	AC-4(19)	Information Flow Enforcement | Validation of Metadata	When transferring information between different security domains, implement [Assignment: organization-defined approved configurations] for control the flow of [Assignment: organization-defined information] across security domains.	AC-4(19)	Not Selected	Functional	Equal	10	Metadata Validation	NET-04.13	Automated mechanisms exist to apply cybersecurity and/or data protection filters on metadata.											AC-4(19)	AC-4(19)						
AC	AC-04(20)	AC-4(20)	Information Flow Enforcement | Approved Solutions	Implement [Assignment: organization-defined solutions] in support of [Assignment: organization-defined information flow control requirements] across [Assignment: organization-defined security domains].	AC-4(20)	Not Selected	Functional	Equal	10	Approved Solutions	NET-04.11	Mechanisms exist to implement approved cybersecurity and data protection solutions for the transfer of information between different security domains, that meet the organization's requirements.																		
AC	AC-04(21)	AC-4(21)	Information Flow Enforcement | Physical or Logical Separation of Information Flows	Separate information flows logically or physically using [Assignment: organization-defined mechanisms and/or techniques] to accomplish [Assignment: organization-defined flow control requirements].	AC-4(21)	Not Selected	Functional	Equal	10	Network Segmentation (macrosegmentation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate Technology Assets, Applications and/or Services (TAAS) to protect from other network resources.						AC-04(21)	AC-04(21)				AC-4(21)					AC-04(21)		AC-04(21)
AC	AC-04(22)	AC-4(22)	Information Flow Enforcement | Access Only	Provide access from a single device to computing platforms, applications, or data residing in multiple different security domains, while preventing information from being transferred between the domains.	AC-4(22)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
AC	AC-04(23)	AC-4(23)	Information Flow Enforcement | Modify Non-releasable Information	When transferring information between different security domains, modify non-releasable information by implementing [Assignment: organization-defined modification actions].	AC-4(23)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
AC	AC-04(24)	AC-4(24)	Information Flow Enforcement | Internal Normalized Format	When transferring information between different security domains, parse incoming data into an internal normalized format and regenerate the data to be consistent with its specified format.	AC-4(24)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
AC	AC-04(25)	AC-4(25)	Information Flow Enforcement | Data Sanitization	When transferring information between different security domains, sanitize data to minimize [Selection (one or more): delivery of malicious content, malicious code augmentation, embedding unauthorized data types, prohibited data types, or prohibited information within data types].	AC-4(25)	Not Selected	Functional	Equal	10	Personal Data Retention & Disposal	PRI-05	Mechanisms exist to: (1) Retain Personal Data (PD), including metadata, for an organization-defined time period to fulfill the purpose(s) identified in the notice or as required by law; (2) Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of storage; and																		
AC	AC-04(26)	AC-4(26)	Information Flow Enforcement | Audit Filtering Actions	When transferring information between different security domains, record and audit content filtering actions and results for the information being transferred as required by [Assignment: organization-defined security policy].	AC-4(26)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
AC	AC-04(27)	AC-4(27)	Information Flow Enforcement | Redundant/Independent Filtering Mechanisms	When transferring information between different security domains, implement content filtering solutions that provide redundant and independent filtering.	AC-4(27)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
AC	AC-04(28)	AC-4(28)	Information Flow Enforcement | Linear Filter Pipelines	When transferring information between different security domains, implement a linear content filter pipeline that is enforced with discretionary and mandatory access controls.	AC-4(28)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
AC	AC-04(29)	AC-4(29)	Information Flow Enforcement | Filter Orchestration Engines	When transferring information between different security domains, ensure that a. Content filtering mechanisms successfully complete execution without errors; and b. Content filtering mechanisms implemented to support [Assignment: organization-defined security policy] are not bypassed or circumvented.	AC-4(29)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
AC	AC-04(30)	AC-4(30)	Information Flow Enforcement | Filter Mechanisms Using Multiple Processes	When transferring information between different security domains, implement content filtering mechanisms using multiple processes.	AC-4(30)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
AC	AC-04(31)	AC-4(31)	Information Flow Enforcement | Failed Content Transfer Prevention	When transferring information between different security domains, prevent the transfer of failed content to the receiving domain.	AC-4(31)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
AC	AC-04(32)	AC-4(32)	Information Flow Enforcement | Process Requirements for Information Transfer	When transferring information between different security domains, implement [Assignment: organization-defined security policy filters] requiring fully enumerated formats that restrict data structure and content.	AC-4(32)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
AC	AC-05	AC-5	Separation of Duties	Validates filtering metadata; and c. Ensures the content filtering mechanisms successfully complete execution without errors.	AC-5	Moderate	Functional	Intersects With	5	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	AC-5	AC-5	AC-5	AC-5	AC-05	AC-05	AC-05	AC-05	AC-5	AC-5	AC-5	AC-5	AC-5		AC-05	AC-05		AC-05
AC	AC-05	AC-5	Separation of Duties	Identify and document [Assignment: organization-defined duties of individuals requiring separation]; and b. Define system access authorizations to support separation of duties.	AC-5	Moderate	Functional	Intersects With	5	Dual Authorization for Change	CHG-04.3	Mechanisms exist to enforce a two-person rule for implementing changes to critical Technology Assets, Applications and/or Services (TAAS).	AC-5

Family	Sorting Control #	Focal Document Element	Focal Document Element Name	Focal Document Element Description	NIST SP 800-53 R5.2	Security Control Baseline	Set Theory Relationship Mapping (STRM)			Reference Document Element	Reference Document Name	Reference Document Element Description	NIST SP 800-53 R5.2 Baselines				FedRAMP R5				CS-CRM Baseline	NIST SP 800-161 R1				GovRAMP				
							Rationale	Relationship	Strength of Relationship				Low	Mod	High	Privacy	Low	Mod	High	LI-SaaS		Down Overlay	Level 1	Level 2	Level 3	Low	Low+	Moderate	Core	High (FedRAMP Inc)
AC	AC-09(01)	AC-9(1)	Previous Logon Notification | Unsuccessful Logons	unsuccessful logon attempts since the last successful	AC-9(1)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
AC	AC-09(02)	AC-9(2)	Previous Logon Notification | Successful and Unsuccessful Logons	Selection (one): successful logons; unsuccessful logon attempts; both] during [Assignment: organization-	AC-9(2)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
AC	AC-09(03)	AC-9(3)	Previous Logon Notification | Notification of Account Changes	[Assignment: organization-defined security-related characteristics or parameters of the user's account]	AC-9(3)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
AC	AC-09(04)	AC-9(4)	Previous Logon Notification | Additional Logon Information	additional information: [Assignment: organization-	AC-9(4)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
AC	AC-10	AC-10	Concurrent Session Control	[Assignment: organization-defined account and/or account type] to [Assignment: organization-defined	AC-10	High	Functional	Equal	10	Concurrent Session Control	IAC-23	Mechanisms exist to limit the number of concurrent sessions for each system account.			AC-10				AC-10									AC-10	
AC	AC-11	AC-11	Device Lock	the user to initiate a device lock before leaving the	AC-11	Moderate	Functional	Intersects With	5	Session Lock	IAC-24	upon receiving a request from a user and retain the session lock until the user reestablishes access		AC-11	AC-11			AC-11	AC-11							AC-11	AC-11		AC-11
AC	AC-11(01)	AC-11(1)	Device Lock | Pattern-hiding Displays	Conceal, via the device lock, information previously visible on the display with a publicly viewable image.	AC-11(1)	Moderate	Functional	Equal	10	Pattern-Hiding Displays	IAC-24.1	Mechanisms exist to implement pattern-hiding displays to conceal information previously visible on the display during the session lock.		AC-11(1)	AC-11(1)			AC-11(01)	AC-11(01)								AC-11(01)	
AC	AC-12	AC-12	Session Termination	[Assignment: organization-defined conditions or trigger	AC-12	Moderate	Functional	Equal	10	Session Termination	IAC-25	Automated mechanisms exist to log out users, both locally on the network and for remote sessions, at the end of the session or after an organization-defined period of inactivity.		AC-12	AC-12			AC-12	AC-12							AC-12	AC-12		AC-12
AC	AC-12(01)	AC-12(1)	Session Termination | User-initiated Logouts	communications sessions whenever authentication is used to gain access to [Assignment: organization-	AC-12(1)	Not Selected	Functional	Equal	10	User-Initiated Logouts / Message Displays	IAC-25.1	Mechanisms exist to provide a logout capability and display an explicit logout message to users indicating the reliable termination of the session.																AC-12(01)
AC	AC-12(02)	AC-12(2)	Session Termination | Termination Message	the termination of authenticated communications	AC-12(2)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
AC	AC-12(03)	AC-12(3)	Session Termination | Timeout Warning Message	session will end in [Assignment: organization-defined	AC-12(3)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
AC	AC-13	AC-13		Withdrawn	AC-13	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																	
AC	AC-14	AC-14	Permitted Actions Without Identification or Authentication	organizational mission and business functions; and]b.	AC-14	Low	Functional	Equal	10	Permitted Actions Without Identification or Authorization	IAC-26	Mechanisms exist to identify and document the supporting rationale for specific user actions that can be performed on a system without identification or authentication.	AC-14	AC-14	AC-14		AC-14	AC-14	AC-14	AC-14						AC-14	AC-14	AC-14		AC-14
AC	AC-14(01)	AC-14(1)		Withdrawn	AC-14(1)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																	
AC	AC-15	AC-15		Withdrawn	AC-15	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																	
AC	AC-16	AC-16	Security and Privacy Attributes	defined in AC-16a for [Assignment: organization-defined systems]; [Assignment: organization-defined security	AC-16	Not Selected	Functional	Equal	10	Cybersecurity & Data Protection Attributes	DCH-05	Mechanisms exist to bind cybersecurity and data protection attributes to information as it is stored, transmitted and processed.																	
AC	AC-16(01)	AC-16(1)	Security and Privacy Attributes | Dynamic Attribute Association	objects] in accordance with the following security and privacy policies as information is created and combined:	AC-16(1)	Not Selected	Functional	Equal	10	Dynamic Attribute Association	DCH-05.1	and objects as information is created, combined, or transformed, in accordance with organization-defined																	
AC	AC-16(02)	AC-16(2)	Security and Privacy Attributes | Attribute Value Changes by Authorized Individuals	behalf of individuals) the capability to define or change	AC-16(2)	Not Selected	Functional	Equal	10	Attribute Value Changes By Authorized Individuals	DCH-05.2	Mechanisms exist to provide authorized individuals (or processes acting on behalf of individuals) the capability to define or change the value of associated cybersecurity and data protection attributes.																	
AC	AC-16(03)	AC-16(3)	Security and Privacy Attributes | Maintenance of Attribute Associations by System	organization-defined security and privacy attributes] to	AC-16(3)	Not Selected	Functional	Equal	10	Maintenance of Attribute Associations By System	DCH-05.3	Mechanisms exist to maintain the association and integrity of cybersecurity and data protection attributes to individuals and objects.																	
AC	AC-16(04)	AC-16(4)	Security and Privacy Attributes | Association of Attributes by Authorized Individuals	with [Assignment: organization-defined subjects and	AC-16(4)	Not Selected	Functional	Equal	10	Association of Attributes By Authorized Individuals	DCH-05.4	Mechanisms exist to provide the capability to associate cybersecurity and data protection attributes with individuals and objects by authorized individuals (or processes acting on behalf of individuals).																	
AC	AC-16(05)	AC-16(5)	Security and Privacy Attributes | Attribute Displays on Objects to Be Output	to output devices to identify [Assignment: organization-	AC-16(5)	Not Selected	Functional	Equal	10	Attribute Displays for Output Devices	DCH-05.5	Mechanisms exist to bind attributes to data stored, transmitted or processed by an information system to enable automated mechanisms to accurately and reliably associate each object that the system transmits to output devices to identify special dissemination, handling or distribution instructions, or security and data protection attributes that are used to enforce information flow restrictions and data protection attributes with individuals and objects in accordance with cybersecurity and data protection policies.																	
AC	AC-16(06)	AC-16(6)	Security and Privacy Attributes | Maintenance of Attribute Association	organization-defined subjects and objects] in accordance	AC-16(6)	Not Selected	Functional	Equal	10	Data Subject Attribute Associations	DCH-05.6	Mechanisms exist to provide a consistent, organizational approach to the interpretation of cybersecurity and data protection attributes employed in access enforcement and flow enforcement decisions																	
AC	AC-16(07)	AC-16(7)	Security and Privacy Attributes | Consistent Attribute Interpretation	privacy attributes transferred between distributed	AC-16(7)	Not Selected	Functional	Equal	10	Consistent Attribute Interpretation	DCH-05.7																		
AC	AC-16(08)	AC-16(8)	Security and Privacy Attributes | Association Techniques and Technologies	techniques and technologies] in associating security and	AC-16(8)	Not Selected	Functional	Equal	10	Identity Association Techniques & Technologies	DCH-05.8	Mechanisms exist to associate cybersecurity and data protection attributes to information.																	
AC	AC-16(09)	AC-16(9)	Security and Privacy Attributes | Attribute Reassignment — Regrading Mechanisms	information only via regrading mechanisms validated	AC-16(9)	Not Selected	Functional	Equal	10	Attribute Reassignment	DCH-05.9	Mechanisms exist to reclassify data as required, due to changing business/technical requirements.																	
AC	AC-16(10)	AC-16(10)	Security and Privacy Attributes | Attribute Configuration by Authorized Individuals	change the type and value of security and privacy	AC-16(10)	Not Selected	Functional	Equal	10	Attribute Configuration By Authorized Individuals	DCH-05.10	Mechanisms exist to provide authorized individuals the capability to define or change the type and value of cybersecurity and data protection attributes available for association with subjects and objects.																	
AC	AC-17	AC-17	Remote Access	implementation guidance for each type of remote access	AC-17	Low	Functional	Intersects With	5	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	AC-17	AC-17	AC-17		AC-17	AC-17	AC-17	AC-17	AC-17					AC-17	AC-17	AC-17	AC-17	AC-17
AC	AC-17(01)	AC-17(1)	Remote Access | Monitoring and Control	Employ automated mechanisms to monitor and control	AC-17(1)	Moderate	Functional	Equal	10	Automated Monitoring & Control	NET-14.1	Automated mechanisms exist to monitor and control remote access sessions.		AC-17(1)	AC-17(1)			AC-17(01)	AC-17(01)							AC-17(01)	AC-17(01)		AC-17(01)
AC	AC-17(02)	AC-17(2)	Remote Access | Protection of Confidentiality and Integrity Using Encryption	implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.	AC-17(2)	Moderate	Functional	Equal	10	Protection of Confidentiality / Integrity Using Encryption	NET-14.2	Cryptographic mechanisms exist to protect the confidentiality and integrity of remote access sessions (e.g., VPN).		AC-17(2)	AC-17(2)			AC-17(02)	AC-17(02)							AC-17(02)	AC-17(02)	AC-17(02)	AC-17(02)
AC	AC-17(03)	AC-17(3)	Remote Access | Managed Access Control Points	Route remote accesses through authorized and	AC-17(3)	Moderate	Functional	Equal	10	Managed Access Control Points	NET-14.3	Mechanisms exist to route all remote accesses through managed network access control points (e.g., VPN concentrator).		AC-17(3)	AC-17(3)			AC-17(03)	AC-17(03)							AC-17(03)			AC-17(03)
AC	AC-17(04)	AC-17(4)	Remote Access | Privileged Commands and Access	evidence and for the following needs: [Assignment:	AC-17(4)	Moderate	Functional	Equal	10	Remote Privileged Commands & Sensitive Data Access	NET-14.4	Mechanisms exist to restrict the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs.		AC-17(4)	AC-17(4)			AC-17(04)	AC-17(04)							AC-17(04)			AC-17(04)
AC	AC-17(05)	AC-17(5)		Withdrawn	AC-17(5)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																	
AC	AC-17(06)	AC-17(6)	Remote Access | Protection of Mechanism Information	Protect information about remote access mechanisms	AC-17(6)	Not Selected	Functional	Intersects With	5	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.										AC-17(6)	AC-17(6)							
AC	AC-17(07)	AC-17(7)		Withdrawn	AC-17(7)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																	
AC	AC-17(08)	AC-17(8)		Withdrawn	AC-17(8)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																	
AC	AC-17(09)	AC-17(9)	Remote Access | Disconnect or Disable Access	access to the system within [Assignment: organization-	AC-17(9)	Not Selected	Functional	Equal	10	Expeditious Disconnect / Disable Capability	NET-14.8	Mechanisms exist to provide the capability to expeditiously disconnect or disable a user's remote access session.														AC-17(09)	AC-17(09)		AC-17(09)
AC	AC-17(10)	AC-17(10)	Remote Access | Authenticate Remote Commands	mechanisms] to authenticate [Assignment: organization-	AC-17(10)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
AC	AC-18	AC-18	Wireless Access	type of wireless access; and]b. Authorize each type of	AC-18	Low	Functional	Intersects With	5	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	AC-18	AC-18	AC-18	AC-18	AC-18	AC-18	AC-18	AC-18	AC-18	AC-18	AC-18	AC-18	AC-18	AC-18	AC-18	AC-18	AC-18
AC	AC-18	AC-18	Wireless Access	type of wireless access; and]b. Authorize each type of	AC-18	Low	Functional	Intersects With	5	Wireless Access Authentication & Encryption	CRY-07	Mechanisms exist to protect wireless access via secure authentication and encryption.	AC-18	AC-18	AC-18	AC-18	AC-18	AC-18	AC-18	AC-18	AC-18	AC-18	AC-18	AC-18	AC-18	AC-18	AC-18	AC-18	AC-18
AC	AC-18(01)	AC-18(1)	Wireless Access | Authentication and Encryption	authentication of [Selection (one or more): users;	AC-18(1)	Moderate	Functional	Equal	10	Authentication & Encryption	NET-15.1	Mechanisms exist to protect wireless access through authentication and strong encryption.		AC-18(1)	AC-18(1)			AC-18(01)	AC-18(01)							AC-18(01)			AC-18(01)
AC	AC-18(02)	AC-18(2)		Withdrawn	AC-18(2)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																	
AC	AC-18(03)	AC-18(3)	Wireless Access | Disable Wireless Networking	capabilities embedded within system components prior	AC-18(3)	Moderate	Functional	Equal	10	Disable Wireless Networking	NET-15.2	Mechanisms exist to disable unnecessary wireless networking capabilities that are internally embedded within system components prior to issuance to end users.		AC-18(3)	AC-18(3)			AC-18(03)	AC-18(03)										AC-18(03)
AC	AC-18(04)	AC-18(4)	Wireless Access | Restrict Configurations by Users	independently configure wireless networking	AC-18(4)	High	Functional	Equal	10	Restrict Configuration By Users	NET-15.3	Mechanisms exist to identify and explicitly authorize users who are allowed to independently configure wireless networking capabilities.			AC-18(4)				AC-18(04)										AC-18(04)
AC	AC-18(05)	AC-18(5)	Wireless Access | Antennas and Transmission Power Levels	levels to reduce the probability that signals from wireless access points can be received outside of	AC-18(5)	High	Functional	Equal	10	Wireless Boundaries	NET-15.4	Mechanisms exist to confine wireless communications to organization-controlled boundaries.			AC-18(5)				AC-18(05)										AC-18(05)
AC	AC-19	AC-19	Access Control for Mobile Devices	such devices are outside of controlled areas; andb.	AC-19	Low	Functional	Equal	10	Access Control For Mobile Devices	MDM-02	Mechanisms exist to enforce access control requirements for the connection of mobile devices to organizational Technology Assets, Applications and/or Services (TAAS).	AC-19	AC-19	AC-19		AC-19	AC-19	AC-19	AC-19	AC-19			AC-19	AC-19	AC-19	AC-19	AC-19	AC-19	AC-19
AC	AC-19(01)	AC-19(1)		Withdrawn	AC-19(1)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																	
AC	AC-19(02)	AC-19(2)		Withdrawn	AC-19(2)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																	
AC	AC-19(03)	AC-19(3)		Withdrawn	AC-19(3)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																	
AC	AC-19(04)	AC-19(4)	Access Control for Mobile Devices | Restrictions for Classified Information	to unclassified systems requires approval from the	AC-19(4)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
AC	AC-19(05)	AC-19(5)	Access Control for Mobile Devices | Full Device or Container-based Encryption	[Selection (one): full-device encryption; container-based encryption] to protect the confidentiality and	AC-19(5)	Moderate	Functional	Equal	10	Full Device & Container-Based Encryption	MDM-03	Cryptographic mechanisms exist to protect the confidentiality and integrity of information on mobile devices through full-device or container encryption.		AC-19(5)	AC-19(5)			AC-19(05)	AC-19(05)							AC-19(05)			AC-19(05)
AC	AC-20	AC-20	Use of External Systems	organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to:	AC-20	Low	Functional	Equal	10	Use of External Information Systems	DCH-13	Mechanisms exist to govern how external parties, including Technology Assets, Applications and/or Services (TAAS), are used to securely store, process and transmit data.	AC-20	AC-20	AC-20		AC-20	AC-20	AC-20	AC-20	AC-20	AC-20	AC-20	AC-20	AC-20	AC-20	AC-20	AC-20	AC-20
AC	AC-20(01)	AC-20(1)	Use of External Systems | Limits on Authorized Use	external system as specified in the organization's	AC-20(1)	Moderate	Functional	Equal	10	Limits of Authorized Use	DCH-13.1	Mechanisms exist to prohibit external parties, including Technology Assets, Applications and/or Services (TAAS), from storing, processing and transmitting data unless authorized individuals first:		AC-20(1)	AC-20(1)			AC-20(01)	AC-20(01)			AC-20(1)	AC-20(1)			AC-20(01)	AC-20(01)		AC-20(01)
AC	AC-20(02)	AC-20(2)	Use of External Systems | Portable Storage Devices — Restricted Use	storage devices by authorized individuals on external systems using [Assignment: organization-defined	AC-20(2)	Moderate	Functional	Intersects With	5	Portable Storage Devices	DCH-13.2	Mechanisms exist to restrict or prohibit the use of portable storage devices by users on external systems.		AC-20(2)	AC-20(2)			AC-20(02)	AC-20(02)							AC-20(02)			AC-20(02)
AC	AC-20(03)	AC-20(3)	Use of External Systems | Non-organizationally Owned Systems — Restricted Use	Use of system components to process, store, or transmit organizational information using [Assignment:	AC-20(3)	Not Selected	Functional	Equal	10	Non-Organizationally Owned Systems / Components / Devices	DCH-13.4	Mechanisms exist to restrict the use of non-organizationally owned Technology Assets, Applications and/or Services (TAAS) to process, store or transmit organizational information.										AC-20(3)	AC-20(3)						
AC	AC-20(04)	AC-20(4)	Use of External Systems | Network Accessible Storage Devices — Prohibited Use	Prohibit the use of [Assignment: organization-defined network accessible storage devices] in external systems.	AC-20(4)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
AC	AC-20(05)	AC-20(5)	Use of External Systems | Portable Storage Devices — Prohibited Use	storage devices by authorized individuals on external	AC-20(5)	Not Selected	Functional	Equal	10	Portable Storage Devices	DCH-13.2	Mechanisms exist to restrict or prohibit the use of portable storage devices by users on external systems.																	
AC	AC-21	AC-21	Information Sharing	[Assignment: organization-defined information sharing circumstances where user discretion is required]; andb.	AC-21	Moderate	Functional	Intersects With	5	Information Sharing With Third Parties	PRI-07	Mechanisms exist to disclose Personal Data (PD) to third-parties only for the purposes identified in the data privacy notice and with the implicit or explicit consent of the data subject.	AC-21	AC-21	AC-21	AC-21	AC-21	AC-21	AC-21	AC-21	AC-21	AC-21	AC-21	AC-21		AC-21	AC-21		AC-21
AC	AC-21	AC-21	Information Sharing	[Assignment: organization-defined information sharing circumstances where user discretion is required]; andb.	AC-21	Moderate	Functional	Intersects With	5	Information Sharing	DCH-14	Mechanisms exist to utilize a process to assist users in making information sharing decisions to ensure data is appropriately protected.	AC-21	AC-21	AC-21	AC-21	AC-21	AC-21	AC-21	AC-21	AC-21	AC-21	AC-21	AC-21		AC-21	AC-21		AC-21
AC	AC-21(01)	AC-21(1)	Information Sharing | Automated Decision Support	by authorized users based on access authorizations of	AC-21(1)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
AC	AC-21(02)	AC-21(2)	Information Sharing | Information Search and Retrieval	enforce [Assignment: organization-defined information	AC-21(2)	Not Selected	Functional	Equal	10	Information Search & Retrieval	DCH-14.1	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) implement data search and retrieval functions that properly enforce data protection / sharing restrictions.																	
AC	AC-22	AC-22	Publicly Accessible Content	content of information prior to posting onto the publicly	AC-22	Low	Functional	Equal	10	Publicly Accessible Content	DCH-15	Mechanisms exist to control publicly-accessible content.	AC-22	AC-22	AC-22		AC-22	AC-22	AC-22	AC-22	AC-22			AC-22	AC-22		AC-22		AC-22
AC	AC-23	AC-23	Data Mining Protection	prevention and detection techniques] for [Assignment:	AC-23	Not Selected	Functional	Intersects With	5	Data Mining Protection	DCH-16	Mechanisms exist to protect data storage objects against unauthorized data mining and data harvesting techniques.	AC-23	AC-23	AC-23	AC-23	AC-23	AC-23	AC-23	AC-23	AC-23	AC-23	AC-23	AC-23					
AC	AC-23	AC-23	Data Mining Protection	prevention and detection techniques] for [Assignment:	AC-23	Not Selected	Functional	Intersects With	5	Usage Restrictions of Sensitive Personal Data	PRI-05.4	Mechanisms exist to restrict the use of Personal Data (PD) to only the authorized purpose(s) consistent with applicable laws, regulations and in data privacy notices.	AC-23	AC-23	AC-23	AC-23	AC-23	AC-23	AC-23	AC-23	AC-23	AC-23	AC-23	AC-23					
AC	AC-24	AC-24	Access Control Decisions	organization-defined access control decisions] are	AC-24	Not Selected	Functional	Intersects With	5	Management Approval For New or Changed Accounts	IAC-28.1	Mechanisms exist to ensure management approvals are required for new accounts or changes in permissions to existing accounts.										AC-24	AC-24	AC-24	AC-24				
AC	AC-24(01)	AC-24(1)	Access Control Decisions | Transmit Access Authorization Information	organization-defined controls] to [Assignment:	AC-24(1)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
AC	AC-24(02)	AC-24(2)	Access Control Decisions | No User or Process Identity	organization-defined security or privacy attributes] that do not include the identity of the user or process acting	AC-24(2)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
AC	AC-25	AC-25	Reference Monitor	tamperproof, always invoked, and small enough to be	AC-25	Not Selected	Functional	Equal	10	Reference Monitor	IAC-27	Mechanisms exist to implement a reference monitor that is tamperproof, always-invoked, small enough to be subject to analysis / testing and the completeness of which can be assured.																	
AT	AT-01	AT-1	Policy and Procedures	implementation of the awareness and training policy and	AT-1	Low	Functional	Intersects With	5	Cybersecurity & Data Protection	GOV-03	Mechanisms exist to review the cybersecurity & data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their	AT-1	AT-1	AT-1	AT-1	AT-01	AT-01	AT-01	AT-01	AT-1	AT-1	AT-1	AT-1	AT-1	AT-01	AT-01	AT-01	AT-01
AT	AT-01	AT-1	Policy and Procedures	implementation of the awareness and training policy and	AT-1	Low	Functional	Subset Of	10	Cybersecurity & Data Protection-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	AT-1	AT-1	AT-1	AT-1	AT-01	AT-01	AT-01	AT-01	AT-1	AT-1	AT-1	AT-1	AT-1	AT-01	AT-01	AT-01	AT-01
AT	AT-01	AT-1	Policy and Procedures	implementation of the awareness and training policy and	AT-1	Low	Functional	Intersects With	5	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	AT-1	AT-1	AT-1	AT-1	AT-01	AT-01	AT-01	AT-01	AT-1	AT-1	AT-1	AT-1	AT-1	AT-01	AT-01	AT-01	AT-01
AT	AT-02	AT-2	Literacy Training and Awareness	and privacy awareness of system users [Assignment:	AT-2	Low	Functional	Equal	10	Cybersecurity & Data Protection Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	AT-2	AT-2	AT-2	AT-2	AT-02	AT-02	AT-02	AT-02						AT-02	AT-02	AT-02	AT-02
AT	AT-02(01)	AT-2(1)	Literacy Training and Awareness | Practical Exercises	Provide practical exercises in literacy training that	AT-2(1)	Not Selected	Functional	Intersects With	5	Simulated Cyber Attack Scenario Training	SAT-02.1	Mechanisms exist to include simulated actual cyber-attacks through practical exercises that are aligned with current threat scenarios.													AT-2(1)				
AT	AT-02(02)	AT-2(2)	Literacy Training and Awareness | Insider Threat	Provide literacy training on recognizing and reporting	AT-2(2)	Low	Functional	Equal	10	Insider Threat Awareness	THR-05	Mechanisms exist to utilize security awareness training on recognizing and reporting potential indicators of insider threat.	AT-2(2)	AT-2(2)	AT-2(2)		AT-02(02)	AT-02(02)	AT-02(02)	AT-02(02)	AT-2(2)	AT-2(2)		AT-2(2)		AT-02(02)	AT-02(02)		AT-02(02)
AT	AT-02(03)	AT-2(3)	Literacy Training and Awareness | Social Engineering and Mining	potential and actual instances of social engineering and	AT-2(3)	Moderate	Functional	Equal	10	Social Engineering & Mining	SAT-02.2	Mechanisms exist to include awareness training on recognizing and reporting potential and actual instances of social engineering and social mining.		AT-2(3)	AT-2(3)			AT-02(03)	AT-02(03)					AT-2(3)					
AT	AT-02(04)	AT-2(4)	Literacy Training and Awareness | Suspicious Communications and Anomalous System Behavior	communications and anomalous behavior in	AT-2(4)	Not Selected	Functional	Intersects With	5	Suspicious Communications & Anomalous System Behavior	SAT-03.2	Mechanisms exist to provide training to personnel on organization-defined indicators of malware to recognize suspicious communications and anomalous behavior.												AT-2(4)					
AT	AT-02(05)	AT-2(5)	Literacy Training and Awareness | Advanced Persistent Threat	Provide literacy training on the advanced persistent threat.	AT-2(5)	Not Selected	Functional	Intersects With	5	Suspicious Communications & Anomalous System Behavior	SAT-03.2	Mechanisms exist to provide training to personnel on organization-defined indicators of malware to recognize suspicious communications and anomalous behavior.												AT-2(5)					
AT	AT-02(06)	AT-2(6)	Literacy Training and Awareness | Cyber Threat Environment	Provide literacy training on the cyber threat environment.	AT-2(6)	Not Selected	Functional	Equal	10	Cyber Threat Environment	SAT-03.6	Mechanisms exist to provide role-based cybersecurity and data protection awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.												AT-2(6)					
AT	AT-03	AT-3	Role-based Training	[Assignment: organization-defined frequency] thereafter; and]c. When required by system changes; and]d. Update role-	AT-3	Low	Functional	Intersects With	5	Role-Based Cybersecurity & Data Protection Training	SAT-03	(1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and	AT-3	AT-3	AT-3	AT-3	AT-03	AT-03	AT-03	AT-03	AT-3	AT-3		AT-3		AT-03	AT-03	AT-03	AT-03
AT	AT-03(01)	AT-3(1)	Role-based Training | Environmental Controls	roles] with initial and [Assignment: organization-defined frequency] training in the employment and operation of	AT-3(1)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
AT	AT-03(02)	AT-3(2)	Role-based Training | Physical Security Controls	roles] with initial and [Assignment: organization-defined frequency] training in the employment and operation of	AT-3(2)	Not Selected	Functional	Intersects With	5	Role-Based Cybersecurity & Data Protection Training	SAT-03	(1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and												AT-3(2)					
AT	AT-03(03)	AT-3(3)	Role-based Training | Practical Exercises	Provide practical exercises in security and privacy training that reinforce training objectives.	AT-3(3)	Not Selected	Functional	Equal	10	Practical Exercises	SAT-03.1	Mechanisms exist to include practical exercises in cybersecurity and data protection training that reinforce training objectives.																	AT-03(03)
AT	AT-03(04)	AT-3(4)		Withdrawn	AT-3(4)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																	AT-03(04)
AT	AT-03(05)	AT-3(5)	Role-based Training | Processing Personally Identifiable Information	frequency] training in the employment and operation of	AT-3(5)	Not Selected	Functional	Equal	10	Sensitive Information Storage, Handling & Processing	SAT-03.3	Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive information is formally trained in data handling requirements.				AT-3(5)													
AT	AT-04	AT-4	Training Records	awareness training and specific role-based security and	AT-4	Low	Functional	Equal	10	Cybersecurity & Data Protection Training Records	SAT-04	Mechanisms exist to document cybersecurity & data protection training activities, including security awareness training and cybersecurity and data protection awareness training, ongoing awareness training and specific-system	AT-4	AT-4	AT-4	AT-4	AT-04	AT-04	AT-04	AT-04	AT-4			AT-4		AT-04	AT-04	AT-04	AT-04
AT	AT-05	AT-5		Withdrawn	AT-5	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																	
AT	AT-06	AT-6	Training Feedback	the following personnel [Assignment: organization-defined frequency]: [Assignment: organization-defined	AT-6	Not Selected	Functional	Intersects With	5	Simulated Cyber Attack Scenario Training	SAT-02.1	Mechanisms exist to include simulated actual cyber-attacks through practical exercises that are aligned with current threat scenarios.																	
AU	AU-01	AU-1	Policy and Procedures	implementation of the audit and accountability policy	AU-1	Low	Functional	Intersects With	5	Cybersecurity & Data Protection	GOV-03	Mechanisms exist to review the cybersecurity & data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their	AU-1	AU-1	AU-1	AU-1	AU-01	AU-01	AU-01	AU-01	AU-1	AU-1	AU-1	AU-1	AU-1	AU-01	AU-01	AU-01	AU-01
AU	AU-01	AU-1	Policy and Procedures	implementation of the audit and accountability policy	AU-1	Low	Functional	Intersects With	5	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	AU-1	AU-1	AU-1	AU-1	AU-01	AU-01	AU-01	AU-01	AU-1	AU-1	AU-1	AU-1	AU-1	AU-01	AU-01	AU-01	AU-01
AU	AU-01	AU-1	Policy and Procedures	implementation of the audit and accountability policy	AU-1	Low	Functional	Subset Of	10	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	AU-1	AU-1	AU-1	AU-1	AU-01	AU-01	AU-01	AU-01	AU-1	AU-1	AU-1	AU-1	AU-1	AU-01	AU-01	AU-01	AU-01
AU	AU-02	AU-2	Event Logging	[Assignment: organization-defined event types (subset	AU-2	Low	Functional	Intersects With	5	Reviews & Updates	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	AU-2	AU-2	AU-2	AU-2	AU-02

Family	Sorting Control #	Focal Document Element	Focal Document Element Description	NIST SP 800-53 R5.2	Security Control Baseline	Set Theory Relationship Mapping (STRM) Rationale	Relationship	Strength of Relationship	Reference Document Element	Reference Document Name	Reference Document Element Description	NIST SP 800-53 R5.2 Baselines Low	Mod	High	Privacy	FedRAMP R5 Low	Mod	High	LI-SaaS	CSCRM Baseline	NIST SP 800-161 R1 Down	Level 1	Level 2	Level 3	GovRAMP Low	Low+	Moderate	Core	High (FedRAMP Int.)
AU	AU-03(01)	AU-3(1)	Content of Audit Records | Additional Audit Information	[Assignment: organization-defined information to be included in addition to event name, time stamp, source, outcome, and identity]	AU-3(1)	Moderate	Functional	Intersects With	5	Sensitive Audit Information	MON-03.1	Mechanisms exist to protect sensitive/regulated data contained in log files.		AU-3(1)	AU-3(1)			AU-03(01)	AU-03(01)								AU-03(01)		AU-03(01)
AU	AU-03(02)	AU-3(2)	Withdrawn		AU-3(2)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		AU-03(02)
AU	AU-03(03)	AU-3(3)	Content of Audit Records | Limit Personally Identifiable Information Elements	audit records to the following elements identified in the privacy risk assessment: [Assignment: organization-defined elements]	AU-3(3)	Not Selected	Functional	Equal	10	Limit Personal Data (PD) in Audit Records	MON-03.5	Mechanisms exist to limit Personal Data (PD) contained in audit records to the elements identified in the data privacy risk assessment.				AU-3(3)													
AU	AU-04	AU-4	Audit Log Storage Capacity	[Assignment: organization-defined audit log retention requirements]	AU-4	Low	Functional	Equal	10	Event Log Storage Capacity	MON-04	Mechanisms exist to allocate and proactively manage sufficient event log storage capacity to reduce the likelihood of such capacity being exceeded.	AU-4	AU-4	AU-4		AU-04	AU-04	AU-04	AU-04						AU-04	AU-04	AU-04		AU-04
AU	AU-04(01)	AU-4(1)	Audit Log Storage Capacity | Transfer to Alternate Storage	[Assignment: organization-defined frequency] to a different system, system component, or media other than the system or system component that conducted logging; and	AU-4(1)	Not Selected	Functional	Intersects With	5	Event Log Backup on Separate Physical Systems / Components	MON-08.1	Mechanisms exist to back up event logs onto a physically different system or system component than the System Incident Event Manager (SIEM) or similar automated tool.																	
AU	AU-05	AU-5	Response to Audit Logging Process Failures	[Assignment: organization-defined time period] in the event of an audit logging process failure; and	AU-5	Low	Functional	Equal	10	Response To Event Log Processing Failures	MON-05	Mechanisms exist to alert appropriate personnel in the event of a log processing failure and take actions to remedy the disruption.	AU-5	AU-5	AU-5		AU-05	AU-05	AU-05	AU-05						AU-05	AU-05	AU-05		AU-05
AU	AU-05(01)	AU-5(1)	Response to Audit Logging Process Failures | Storage Capacity Warning	[Assignment: organization-defined time period] when allocated audit log storage volume reaches [Assignment: organization-defined percentage] of repository maximum audit log storage capacity.	AU-5(1)	High	Functional	Equal	10	Event Log Storage Capacity Alerting	MON-05.2	Automated mechanisms exist to alert appropriate personnel when the allocated volume reaches an organization-defined percentage of maximum event log storage capacity.			AU-5(1)				AU-05(01)										AU-05(01)
AU	AU-05(02)	AU-5(2)	Response to Audit Logging Process Failures | Real-time Alerts	[Assignment: organization-defined personnel, roles, and/or locations] when the following audit failure events occur: [Assignment: organization-defined audit failure events requiring real-time alerts].	AU-5(2)	High	Functional	Intersects With	5	Real-Time Alerts of Event Logging Failures	MON-05.1	Mechanisms exist to provide 24x7x365 near real-time alerting capability when an event log processing failure occurs.			AU-5(2)				AU-05(02)										AU-05(02)
AU	AU-05(03)	AU-5(3)	Response to Audit Logging Process Failures | Configurable Traffic Volume Thresholds	[Assignment: organization-defined audit logging traffic volume thresholds reflecting limits on audit log storage capacity and [Selection: reject; delay] network traffic above those thresholds].	AU-5(3)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
AU	AU-05(04)	AU-5(4)	Response to Audit Logging Process Failures | Shutdown on Failure	[Assignment: organization-defined audit logging capability] and [Assignment: organization-defined actions] in the event of an audit logging process failure, unless an alternate audit logging capability exists.	AU-5(4)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
AU	AU-05(05)	AU-5(5)	Response to Audit Logging Process Failures | Alternate Audit Logging Capability	[Assignment: organization-defined alternate audit logging capability] in the event of a failure in primary audit logging capability that implements [Assignment: organization-defined audit log types].	AU-5(5)	Not Selected	Functional	Equal	10	Alternate Event Logging Capability	MON-13	Mechanisms exist to provide an alternate event logging capability in the event of a failure in primary audit capability.																	
AU	AU-06	AU-6	Audit Record Review, Analysis, and Reporting	findings to [Assignment: organization-defined personnel or roles].	AU-6	Low	Functional	Intersects With	5	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM) or similar automated tool, to support the centralized collection of security-related event logs.	AU-6	AU-6	AU-6	AU-6	AU-06	AU-06	AU-06	AU-06	AU-6	AU-6	AU-6	AU-6	AU-6	AU-06	AU-06	AU-06		AU-06
AU	AU-06	AU-6	Audit Record Review, Analysis, and Reporting	findings to [Assignment: organization-defined personnel or roles]; and [Assignment: organization-defined time period].	AU-6	Low	Functional	Intersects With	5	Audit Level Adjustments	MON-02.6	Mechanisms exist to adjust the level of audit review, analysis and reporting based on evolving threat information from law enforcement, industry associations or other credible sources of threat intelligence.	AU-6	AU-6	AU-6	AU-6	AU-06	AU-06	AU-06	AU-06	AU-6	AU-6	AU-6	AU-6	AU-6	AU-06	AU-06	AU-06		AU-06
AU	AU-06(01)	AU-6(1)	Audit Record Review, Analysis, and Reporting | Automated Process Integration	processes using [Assignment: organization-defined automated mechanisms].	AU-6(1)	Moderate	Functional	Intersects With	5	Sensitive Audit Information	MON-03.1	Mechanisms exist to protect sensitive/regulated data contained in log files.						AU-06(01)	AU-06(01)								AU-06(01)		AU-06(01)
AU	AU-06(02)	AU-6(2)		Withdrawn	AU-6(2)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																	
AU	AU-06(03)	AU-6(3)	Audit Record Review, Analysis, and Reporting | Correlate Audit Record Repositories	repositories to gain organization-wide situational awareness.	AU-6(3)	Moderate	Functional	Intersects With	5	Correlate Monitoring Information	MON-02.1	Mechanisms exist to correlate monitoring information from more than one location within the environment with information obtained from other sources to gain enterprise-wide situational awareness.		AU-6(3)	AU-6(3)			AU-06(03)	AU-06(03)									AU-06(03)		AU-06(03)
AU	AU-06(04)	AU-6(4)	Audit Record Review, Analysis, and Reporting | Central Review and Analysis	and analyze audit records from multiple components within the system.	AU-6(4)	Not Selected	Functional	Equal	10	Central Review & Analysis	MON-02.2	Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources.							AU-06(04)										AU-06(04)
AU	AU-06(05)	AU-6(5)	Audit Record Review, Analysis, and Reporting | Integrated Analysis of Audit Records	information; [Assignment: organization-defined information]; and [Assignment: organization-defined vulnerability information].	AU-6(5)	High	Functional	Equal	10	Integration of Scanning & Other Monitoring Information	MON-02.3	Mechanisms exist to integrate the analysis of audit records with the analysis of vulnerability scanners, network performance, system monitoring and other sources to further enhance the ability to identify inappropriate or unusual activity.			AU-6(5)				AU-06(05)										AU-06(05)
AU	AU-06(06)	AU-6(6)	Audit Record Review, Analysis, and Reporting | Correlation with Physical Monitoring	information obtained from monitoring physical access to further enhance the ability to identify suspicious,	AU-6(6)	High	Functional	Equal	10	Correlation with Physical Monitoring	MON-02.4	Automated mechanisms exist to correlate information from monitoring physical access to further enhance the ability to identify suspicious, inappropriate,			AU-6(6)				AU-06(06)										AU-06(06)
AU	AU-06(07)	AU-6(7)	Audit Record Review, Analysis, and Reporting | Permitted Actions	more): system process; role; user] associated with the review, analysis, and reporting of audit record	AU-6(7)	Not Selected	Functional	Equal	10	Permitted Actions	MON-02.5	Mechanisms exist to specify the permitted actions for both users and Technology Assets, Applications and/or Services (TAAS) associated with the review, analysis and reporting of audit information.							AU-06(07)										AU-06(07)
AU	AU-06(08)	AU-6(8)	Audit Record Review, Analysis, and Reporting | Full Text Analysis of Privileged Commands	commands in a physically distinct component or subsystem of the system, or other system that is	AU-6(8)	Not Selected	Functional	Equal	10	Privileged Functions Logging	MON-03.3	Mechanisms exist to log and review the actions of users and/or services with elevated privileges.																	
AU	AU-06(09)	AU-6(9)	Audit Record Review, Analysis, and Reporting | Correlation with Information from Nontechnical Sources	audit record information to enhance cross-organization-wide situational awareness.	AU-6(9)	Not Selected	Functional	Intersects With	5	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate monitoring information from more than one location within the environment with information obtained from other sources to gain enterprise-wide situational awareness.											AU-6(9)						
AU	AU-06(10)	AU-6(10)		Withdrawn	AU-6(10)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																	AU-06(10)
AU	AU-07	AU-7	Audit Record Reduction and Report Generation	audit record review, analysis, and reporting requirements and after-the-fact investigations of	AU-7	Moderate	Functional	Intersects With	5	Monitoring Reporting	MON-06	Mechanisms exist to provide an event log report generation capability to aid in detecting and assessing anomalous activities.		AU-7	AU-7			AU-07	AU-07									AU-07	AU-07	AU-07
AU	AU-07(01)	AU-7(1)	Audit Record Reduction and Report Generation | Automatic Processing	and search audit records for events of interest based on the following content: [Assignment: organization-defined	AU-7(1)	Moderate	Functional	Intersects With	5	Monitoring Reporting	MON-06	Mechanisms exist to provide an event log report generation capability to aid in detecting and assessing anomalous activities.		AU-7(1)	AU-7(1)			AU-07(01)	AU-07(01)									AU-07(01)	AU-07(01)	AU-07(01)
AU	AU-07(02)	AU-7(2)		Withdrawn	AU-7(2)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																	
AU	AU-08	AU-8	Time Stamps	granularity of time measurements] and that use	AU-8	Low	Functional	Intersects With	5	Clock Synchronization	SEA-20	Mechanisms exist to utilize time-synchronization technology to synchronize all critical system clocks.	AU-8	AU-8	AU-8	AU-8	AU-08	AU-08	AU-08	AU-08	AU-8	AU-8	AU-8	AU-8	AU-8	AU-08	AU-08	AU-08		AU-08
AU	AU-08	AU-8	Time Stamps	granularity of time measurements] and that use	AU-8	Low	Functional	Intersects With	5	Time Stamps	MON-07	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to use an authoritative time source to generate time stamps for event logs.	AU-8	AU-8	AU-8	AU-8	AU-08	AU-08	AU-08	AU-08	AU-8	AU-8	AU-8	AU-8	AU-8	AU-08	AU-08	AU-08		AU-08
AU	AU-08(01)	AU-8(1)		Withdrawn	AU-8(1)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A														AU-08(01)	AU-08(01)	AU-08(01)		AU-08(01)
AU	AU-08(02)	AU-8(2)		Withdrawn	AU-8(2)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																	
AU	AU-09	AU-9	Protection of Audit Information	Alert [Assignment: organization-defined personnel or	AU-9	Low	Functional	Equal	10	Protection of Event Logs	MON-08	Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion.	AU-9	AU-9	AU-9		AU-09	AU-09	AU-09	AU-09						AU-09	AU-09	AU-09		AU-09
AU	AU-09(01)	AU-9(1)	Protection of Audit Information | Hardware Write-once Media	write audit trails to hardware-enforced, write-once media.	AU-9(1)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
AU	AU-09(02)	AU-9(2)	Protection of Audit Information | Store on Separate Physical Systems or Components	frequency] in a repository that is part of a physically different system or system component than the system	AU-9(2)	High	Functional	Equal	10	Event Log Backup on Separate Physical Systems / Components	MON-08.1	Mechanisms exist to back up event logs onto a physically different system or system component than the Security Incident Event Manager (SIEM) or similar automated tool.			AU-9(2)				AU-09(02)									AU-09(02)		AU-09(02)
AU	AU-09(03)	AU-9(3)	Protection of Audit Information | Cryptographic Protection	implement cryptographic mechanisms to protect the integrity of audit information and audit tools.	AU-9(3)	High	Functional	Equal	10	Cryptographic Protection of Event Log Information	MON-08.3	Cryptographic mechanisms exist to protect the integrity of event logs and audit tools.			AU-9(3)				AU-09(03)										AU-09(03)
AU	AU-09(04)	AU-9(4)	Protection of Audit Information | Access by Subset of Privileged Users	functionality to only [Assignment: organization-defined subset of privileged users or roles].	AU-9(4)	Moderate	Functional	Equal	10	Access by Subset of Privileged Users	MON-08.2	Mechanisms exist to restrict access to the management of event logs to privileged users with a specific business need.		AU-9(4)	AU-9(4)			AU-09(04)	AU-09(04)									AU-09(04)		AU-09(04)
AU	AU-09(05)	AU-9(5)	Protection of Audit Information | Dual Authorization	movement; deletion] of [Assignment: organization-defined audit information].	AU-9(5)	Not Selected	Functional	Equal	10	Dual Authorization for Event Log Movement	MON-08.4	Automated mechanisms exist to enforce dual authorization for the movement or deletion of event logs.																	
AU	AU-09(06)	AU-9(6)	Protection of Audit Information | Read-only Access	Assignment: organization-defined subset of privileged	AU-9(6)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
AU	AU-09(07)	AU-9(7)	Protection of Audit Information | Store on Component with Different Operating System	[Assignment: organization-defined audit information] on a component running a different operating system than the system or	AU-9(7)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
AU	AU-10	AU-10	Non-repudiation	process acting on behalf of an individual) has performed [Assignment: organization-defined actions to be covered	AU-10	High	Functional	Equal	10	Non-Repudiation	MON-09	Mechanisms exist to utilize a non-repudiation capability to protect against an individual falsely denying having performed a particular action.			AU-10				AU-10				AU-10						AU-10
AU	AU-10(01)	AU-10(1)	Non-repudiation | Association of Identities	[Selection (one or more): validate; maintain] the binding of [Assignment: organization-defined identities] and the information produced by	AU-10(1)	Not Selected	Functional	Intersects With	5	Identity Binding	MON-09.1	Mechanisms exist to bind the identity of the information producer to the information generated.										AU-10(1)						
AU	AU-10(02)	AU-10(2)	Non-repudiation | Validate Binding of Information Producer Identity	[Assignment: organization-defined frequency]; and b. Perform [Assignment: organization-defined actions] in response to	AU-10(2)	Not Selected	Functional	Intersects With	5	Identity Binding	MON-09.1	Mechanisms exist to bind the identity of the information producer to the information generated.										AU-10(2)	AU-10(2)					
AU	AU-10(03)	AU-10(3)	Non-repudiation | Chain of Custody	established chain of custody for information reviewed or produced.	AU-10(3)	Not Selected	Functional	Intersects With	5	Chain of Custody & Forensics	IRO-08	Mechanisms exist to perform digital forensics and maintain the integrity of the chain of custody, in accordance with applicable laws, regulations and industry-recognized secure practices.										AU-10(3)	AU-10(3)					
AU	AU-10(04)	AU-10(4)	Non-repudiation | Validate Binding of Information Reviewer Identity	points prior to release or transfer between [Assignment: organization-defined security domains]; and b. Perform	AU-10(4)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
AU	AU-10(05)	AU-10(5)		Withdrawn	AU-10(5)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																	
AU	AU-11	AU-11	Audit Record Retention	[Assignment: organization-defined time period consistent with records retention policy] to provide support for after-the-fact	AU-11	Low	Functional	Equal	10	Event Log Retention	MON-10	Mechanisms exist to retain event logs for a time period consistent with records retention requirements to provide support for after-the-fact investigations of security incidents and to meet statutory,	AU-11	AU-11	AU-11	AU-11	AU-11	AU-11	AU-11	AU-11						AU-11	AU-11	AU-11	AU-11	AU-11
AU	AU-11(01)	AU-11(1)	Audit Record Retention | Long-term Retrieval Capability	[Assignment: organization-defined measures] are employed to ensure that long-term audit records generated by the	AU-11(1)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
AU	AU-12	AU-12	Audit Record Generation	[Assignment: organization-defined system components]; b. Allow [Assignment: organization-defined personnel or roles] to select the event types that are to	AU-12	Low	Functional	Intersects With	5	Monitoring Reporting	MON-06	Mechanisms exist to provide an event log report generation capability to aid in detecting and assessing anomalous activities.	AU-12	AU-12	AU-12		AU-12	AU-12	AU-12	AU-12	AU-12	AU-12		AU-12	AU-12	AU-12	AU-12	AU-12	AU-12		AU-12
AU	AU-12(01)	AU-12(1)	System-wide and Time-correlated Audit Trail	or physical) audit trail that is time-correlated to within [Assignment: organization-defined level of tolerance for	AU-12(1)	High	Functional	Equal	10	System-Wide / Time-Correlated Audit Trail	MON-02.7	Automated mechanisms exist to compile audit records into an organization-wide audit trail that is time-correlated.			AU-12(1)			AU-12(01)										AU-12(01)
AU	AU-12(02)	AU-12(2)	Audit Record Generation | Standardized Formats	Produce a system-wide (logical or physical) audit trail composed of audit records in a standardized format.	AU-12(2)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
AU	AU-12(03)	AU-12(3)	Audit Record Generation | Changes by Authorized Individuals	ongoing to be performed on [Assignment: organization-defined system components] based on [Assignment:	AU-12(3)	High	Functional	Equal	10	Changes by Authorized Individuals	MON-02.8	Mechanisms exist to provide privileged users or roles the capability to change the auditing to be performed on specified system components, based on specific event criteria within specified time			AU-12(3)				AU-12(03)										AU-12(03)
AU	AU-12(04)	AU-12(4)	Audit Record Generation | Query Parameter Audits of Personally Identifiable Information	parameters of user query events for data sets containing	AU-12(4)	Not Selected	Functional	Equal	10	Query Parameter Audits of Personal Data (PD)	MON-06.1	Mechanisms exist to provide and implement the capability for auditing the parameters of user query events for data sets containing Personal Data (PD).																	
AU	AU-13	AU-13	Monitoring for Information Disclosure	information; and b. If an information disclosure is	AU-13	Not Selected	Functional	Equal	10	Monitoring For Information Disclosure	MON-11	Mechanisms exist to monitor for evidence of unauthorized exfiltration or disclosure of non-public information.					AU-13					AU-13	AU-13						
AU	AU-13(01)	AU-13(1)	Monitoring for Information Disclosure | Use of Automated Tools	using [Assignment: organization-defined automated	AU-13(1)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
AU	AU-13(02)	AU-13(2)	Monitoring for Information Disclosure | Review of Monitored Sites	monitored [Assignment: organization-defined	AU-13(2)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
AU	AU-13(03)	AU-13(3)	Monitoring for Information Disclosure | Unauthorized Replication of Information	determine if external entities are replicating	AU-13(3)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
AU	AU-14	AU-14	Session Audit	circumstances]; and b. Develop, integrate, and use	AU-14	Not Selected	Functional	Equal	10	Session Audit	MON-12	(1) Capture and log all content related to a user session; and								AU-14		AU-14	AU-14						
AU	AU-14(01)	AU-14(1)	Session Audit | System Start-up	Initiate session audits automatically at system start-up.	AU-14(1)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
AU	AU-14(02)	AU-14(2)		Withdrawn	AU-14(2)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																	
AU	AU-14(03)	AU-14(3)	Session Audit | Remote Viewing and Listening	users to remotely view and hear content related to an	AU-14(3)	Not Selected	Functional	Equal	10	Real-Time Session Monitoring	MON-01.17	to an established user session in real time, in accordance with organizational standards, as well as																	
AU	AU-15	AU-15		Withdrawn	AU-15	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																	
AU	AU-16	AU-16	Cross-organizational Audit Logging	information] among external organizations when audit	AU-16	Not Selected	Functional	Intersects With	5	Cross-Organizational Monitoring	MON-14	anomalous events when event logs are shared across organizational boundaries, without giving away										AU-16	AU-16						
AU	AU-16(01)	AU-16(1)	Cross-organizational Audit Logging | Identity Preservation	Preserve the identity of individuals in cross-organizational audit trails.	AU-16(1)	Not Selected	Functional	Intersects With	5	Cross-Organizational Monitoring	MON-14	anomalous events when event logs are shared across organizational boundaries, without giving away																	
AU	AU-16(02)	AU-16(2)	Cross-organizational Audit Logging | Sharing of Audit Information	[Assignment: organization-defined organizations] based on [Assignment: organization-defined cross-	AU-16(2)	Not Selected	Functional	Equal	10	Sharing of Event Logs	MON-14.1	Mechanisms exist to share event logs with third-party organizations based on specific cross-organizational sharing agreements.								AU-16(2)		AU-16(2)	AU-16(2)						
AU	AU-16(03)	AU-16(3)	Cross-organizational Audit Logging | Disassociability	to disassociate individuals from audit information	AU-16(3)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
CA	CA-01	CA-1	Policy and Procedures	and monitoring policy and the associated assessment,	CA-1	Low	Functional	Subset Of	10	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection assessment and authorization controls.	CA-1	CA-1	CA-1	CA-1	CA-01	CA-01	CA-01	CA-01	CA-1	CA-1	CA-1	CA-1	CA-1	CA-01	CA-01	CA-01		CA-01
CA	CA-01	CA-1	Policy and Procedures	and monitoring policy and the associated assessment,	CA-1	Low	Functional	Intersects With	5	Cybersecurity & Data Protection	GOV-03	Mechanisms exist to review the cybersecurity & data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their	CA-1	CA-1	CA-1	CA-1	CA-01	CA-01	CA-01	CA-01	CA-1	CA-1	CA-1	CA-1	CA-1	CA-01	CA-01	CA-01		CA-01
CA	CA-01	CA-1	Policy and Procedures	and monitoring policy and the associated assessment,	CA-1	Low	Functional	Intersects With	5	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	CA-1	CA-1	CA-1	CA-1	CA-01	CA-01	CA-01	CA-01	CA-1	CA-1	CA-1	CA-1	CA-1	CA-01	CA-01	CA-01		CA-01
CA	CA-02	CA-2	Control Assessments	designated representative prior to conducting the	CA-2	Low	Functional	Intersects With	5	Functional Review Of Cybersecurity & Data Protection Controls	CPL-03.2	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's cybersecurity and data protection policies and standards.	CA-2	CA-2	CA-2	CA-2	CA-02	CA-02	CA-02	CA-02	CA-2	CA-2	CA-2	CA-2	CA-2	CA-02	CA-02	CA-02		CA-02
CA	CA-02	CA-2	Control Assessments	designated representative prior to conducting the	CA-2	Low	Functional	Intersects With	5	Technical Verification	IAO-06	Mechanisms exist to perform Information Assurance Program (IAP) activities to evaluate the design, implementation and effectiveness of technical cybersecurity and data protection controls.	CA-2	CA-2	CA-2	CA-2	CA-02	CA-02	CA-02	CA-02	CA-2	CA-2	CA-2	CA-2	CA-2	CA-02	CA-02	CA-02		CA-02
CA	CA-02	CA-2	Control Assessments	designated representative prior to conducting the	CA-2	Low	Functional	Intersects With	5	Cybersecurity & Data Protection In Project Management	PRM-04	Mechanisms exist to assess cybersecurity and data protection controls in system project development to determine the extent to which the controls are implemented correctly, operating as intended and	CA-2	CA-2	CA-2	CA-2	CA-02	CA-02	CA-02	CA-02	CA-2	CA-2	CA-2	CA-2	CA-2	CA-02	CA-02	CA-02		CA-02
CA	CA-02	CA-2	Control Assessments	designated representative prior to conducting the	CA-2	Low	Functional	Intersects With	5	Assessments	IAO-02	Mechanisms exist to formally assess the cybersecurity and data protection controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to	CA-2	CA-2	CA-2	CA-2	CA-02	CA-02	CA-02	CA-02	CA-2	CA-2	CA-2	CA-2	CA-2	CA-02	CA-02	CA-02		CA-02
CA	CA-02	CA-2	Control Assessments	designated representative prior to conducting the	CA-2	Low	Functional	Intersects With	5	Cybersecurity & Data Protection Assessments	CPL-03	within their area of responsibility to adhere to appropriate cybersecurity and data protection policies,	CA-2	CA-2	CA-2	CA-2	CA-02	CA-02	CA-02	CA-02	CA-2	CA-2	CA-2	CA-2	CA-2	CA-02	CA-02	CA-02		CA-02
CA	CA-02(01)	CA-2(1)	Control Assessments | Independent Assessors	employ independent assessors or assessment teams to conduct control assessments.	CA-2(1)	Moderate	Functional	Equal	10	Assessor Independence	IAO-02.1	Mechanisms exist to ensure assessors or assessment teams have the appropriate independence to conduct cybersecurity and data protection control assessments.		CA-2(1)	CA-2(1)		CA-02(01)	CA-02(01)	CA-02(01)	CA-02(01)						CA-02(01)	CA-02(01)	CA-02(01)		CA-02(01)
CA	CA-02(02)	CA-2(2)	Control Assessments | Specialized Assessments	security test cases; vulnerability scanning; malicious	CA-2(2)	High	Functional	Intersects With	5	Specialized Assessments	IAO-02.2	(5) Application security; (6) Embedded technologies (e.g., IoT, OT, etc.);			CA-2(2)				AU-02(02)			CA-2(2)				AU-02(02)		CA-02(02)	
CA	CA-02(03)	CA-2(3)	Control Assessments | Leveraging Results from External Organizations	organization(s)] on [Assignment: organization-defined	CA-2(3)	Not Selected	Functional	Equal	10	Third-Party Assessments	IAO-02.3	Mechanisms exist to accept and respond to the results of external assessments that are performed by impartial, external organizations.						CA-02(03)	CA-02(03)				CA-2(3)				CA-02(03)		CA-02(03)	
CA	CA-03	CA-3	Information Exchange	agreements; [Assignment: organization-defined type of agreement]]; b. Document, as part of each exchange	CA-3	Low	Functional	Intersects With	5	System Interconnections	NET-05	Security Agreements (ISAs), or similar methods, that document, for each interconnection, the interface characteristics, cybersecurity and data protection requirements and the nature of the information	CA-3	CA-3	CA-3		CA-03	CA-03	CA-03	CA-03	CA-3	CA-3			CA-3	CA-03	CA-03	CA-03		CA-03
CA	CA-03(01)	CA-3(1)		Withdrawn	CA-3(1)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																	
CA	CA-03(02)	CA-3(2)		Withdrawn	CA-3(2)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																	
CA	CA-03(03)	CA-3(3)		Withdrawn	CA-3(3)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																	
CA	CA-03(04)	CA-3(4)		Withdrawn	CA-3(4)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																	
CA	CA-03(05)	CA-3(5)		Withdrawn	CA-3(5)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																CA-03(05)		CA-03(05)
CA	CA-03(06)	CA-3(6)	Information Exchange | Transfer Authorizations	between interconnecting systems have the requisite authorizations (i.e., write permissions or privileges) prior	CA-3(6)	High	Functional	Equal	10	Transfer Authorizations	DCH-14.2	Mechanisms exist to verify that individuals or Technology Assets, Applications and/or Services (TAAS) transferring data between interconnecting TAAS have the requisite authorizations (e.g., write			CA-3(6)				CA-03(06)												
CA	CA-03(07)	CA-3(7)	Information Exchange | Transitive Information Exchanges	identified in CA-3a; and b. Take measures to ensure that transitive (downstream) information exchanges cease	CA-3(7)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
CA	CA-04	CA-4		Withdrawn	CA-4	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																	
CA	CA-05	CA-5	Plan of Action and Milestones	reduce or eliminate known vulnerabilities in the system;	CA-5	Low	Functional	Intersects With	5	Plan of Action & Milestones (POA&M)	IAO-05	Mechanisms exist to document planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities.	CA-5	CA-5	CA-5	CA-5	CA-05	CA-05	CA-05	CA-05	CA-5			CA-5	CA-5	CA-05	CA-05	CA-05		CA-05
CA	CA-05(01)	CA-5(1)	Plan of Action and Milestones | Automation Support for Accuracy and Currency	plan of action and milestones for the system using [Assignment: organization-defined automated	CA-5(1)	Not Selected	Functional	Equal	10	Plan of Action & Milestones (POA&M) Automation	IAO-05.1	Automated mechanisms exist to help ensure the Plan of Action and Milestones (POA&M), or similar risk register, is accurate, up-to-date and readily-available.																	
CA	CA-06	CA-6	Authorization	Assign the use of common controls inherited by the	CA-6	Low	Functional	Equal	10	Security Authorization	IAO-07	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.	CA-6	CA-6	CA-6	CA-6	CA-06	CA-06	CA-06	CA-06	CA-6		CA-6	CA-6	CA-6	CA-06	CA-06	CA-06		CA-06
CA	CA-06(01)	CA-6(1)	Authorization | Joint Authorization — Intra-organization	employ a joint authorization process that includes multiple authorizing officials from the same	CA-6(1)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
CA	CA-06(02)	CA-6(2)	Authorization | Joint Authorization — Inter-organization	includes multiple authorizing officials with at least one authorizing official from an organization external to the	CA-6(

Family	Sorting Control #	Focal Document Element	Focal Document Element Name	Focal Document Element Description	NIST SP 800-53 R5.2	Security Control Baseline	Set Theory Relationship Mapping (STRM) Rationale	Set Theory Relationship Mapping (STRM) Relationship	Set Theory Relationship Mapping (STRM) Strength of Relationship	Reference Document Element	Reference Document Name	Reference Document Element Description	NIST SP 800-53 R5.2 Baselines Low	NIST SP 800-53 R5.2 Baselines Mod	NIST SP 800-53 R5.2 Baselines High	NIST SP 800-53 R5.2 Baselines Privacy	FedRAMP R5 Low	FedRAMP R5 Mod	FedRAMP R5 High	FedRAMP R5 LI-SaaS	NIST SP 800-161 R1 C-SCRM Baseline	NIST SP 800-161 R1 Shut Down Systems	NIST SP 800-161 R1 Level 1	NIST SP 800-161 R1 Level 2	NIST SP 800-161 R1 Level 3	GovRAMP Low	GovRAMP Low+	GovRAMP Moderate	GovRAMP Core	GovRAMP High (FedRAMP Hi)
CA	CA-07(06)	CA-7(6)	Continuous Monitoring | Automation Support for Monitoring	[Withdrawn: Incorporated into CA-7.]	CA-7(6)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																			
CA	CA-08	CA-8	Penetration Testing	Conduct penetration testing [Assignment: organization-defined frequency] on [Assignment: organization-defined system or system component] to identify vulnerabilities and document the results.	CA-8	High	Functional	Equal	10	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).			CA-8		CA-08	CA-08	CA-08	CA-08							CA-08	CA-08		CA-08
CA	CA-08(01)	CA-8(1)	Penetration Testing | Independent Penetration Testing Agent or Team	Employ an independent penetration-testing agent or team to perform penetration testing on the system or system components.	CA-8(1)	High	Functional	Equal	10	Independent Penetration Agent or Team	VPM-07.1	Mechanisms exist to utilize an independent assessor or penetration team to perform penetration testing.						CA-8(01)	CA-8(01)								CA-8(01)	CA-8(01)		CA-8(01)
CA	CA-08(02)	CA-8(2)	Penetration Testing | Red Team Exercises	Employ [Assignment: organization-defined red-team exercises] to simulate attempts by adversaries to compromise systems in accordance with applicable rules of engagement.	CA-8(2)	Not Selected	Functional	Equal	10	Red Team Exercises	VPM-10	Mechanisms exist to utilize "red team" exercises to simulate attempts by adversaries to compromise Technology Assets, Applications and/or Services (TAAS) in accordance with organization-defined rules of engagement.						CA-8(02)	CA-8(02)											
CA	CA-08(03)	CA-8(3)	Penetration Testing | Facility Penetration Testing	Employ an independent penetration agent or penetration team to perform penetration testing of [Assignment: organization-defined facilities, systems, or system components within the facilities] to validate physical access controls are effective and resistant to unauthorized physical access attempts, including [Assignment: organization-defined physical access attempts (e.g., tailgating, lock picking, circumventing locks, disabling alarms, cloning badges)].	CA-8(3)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
CA	CA-09	CA-9	Internal System Connections	a. Authorize internal connections of [Assignment: organization-defined system components or classes of components (e.g., digital and non-digital media, laptops, desktops, printers, copiers, scanners, facsimile machines, sensors, servers)] to the system; b. Document, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated; c. Terminate internal system connections after [Assignment: organization-defined conditions]; and d. Review [Assignment: organization-defined frequency] the continued need for each internal connection.	CA-9	Low	Functional	Equal	10	Internal System Connections	NET-05.2	Mechanisms exist to control internal system connections through authorizing internal connections of systems and documenting, for each internal connection, the interface characteristics, security requirements and the nature of the information communicated.	CA-9	CA-9	CA-9		CA-09	CA-09	CA-09	CA-09						CA-09	CA-09	CA-09		CA-09
CA	CA-09(01)	CA-9(1)	Internal System Connections | Compliance Checks	Prohibit the connection of [Assignment: organization-defined constituent system components] to the system unless the component is [Assignment: organization-defined compliant].	CA-9(1)	Not Selected	Functional	Equal	10	Endpoint Security Validation	NET-14.7	Automated mechanisms exist to validate the security posture of the endpoint devices (e.g., software versions, patch levels, etc.) prior to allowing devices to connect to organizational Technology Assets, Applications and/or Services (TAAS).																		
CM	CM-01	CM-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Assignment: organization-defined configuration management policy] that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. [Assignment: organization-defined procedures] to facilitate the implementation of the configuration management policy and the associated configuration management controls; b. Designate an [Assignment: organization-defined official] to manage the configuration management policy and procedures; c. Review and update the configuration management policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and d. Review and update the configuration management procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	CM-1	Low	Functional	Subset Of	10	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	CM-1	CM-1	CM-1	CM-1	CM-01	CM-01	CM-01	CM-01	CM-1	CM-1	CM-1	CM-1	CM-1	CM-01	CM-01	CM-01		CM-01
CM	CM-01	CM-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Assignment: organization-defined configuration management policy] that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. [Assignment: organization-defined procedures] to facilitate the implementation of the configuration management policy and the associated configuration management controls; b. Designate an [Assignment: organization-defined official] to manage the configuration management policy and procedures; c. Review and update the configuration management policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and d. Review and update the configuration management procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	CM-1	Low	Functional	Intersects With	5	Cybersecurity & Data Protection Governance Program	GOV-03	Mechanisms exist to develop, report on and review the organization's cybersecurity and data protection program to standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	CM-1	CM-1	CM-1	CM-1	CM-01	CM-01	CM-01	CM-01	CM-1	CM-1	CM-1	CM-1	CM-1	CM-01	CM-01	CM-01		CM-01
CM	CM-01	CM-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Assignment: organization-defined configuration management policy] that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. [Assignment: organization-defined procedures] to facilitate the implementation of the configuration management policy and the associated configuration management controls; b. Designate an [Assignment: organization-defined official] to manage the configuration management policy and procedures; c. Review and update the configuration management policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and d. Review and update the configuration management procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	CM-1	Low	Functional	Intersects With	5	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	CM-1	CM-1	CM-1	CM-1	CM-01	CM-01	CM-01	CM-01	CM-1	CM-1	CM-1	CM-1	CM-1	CM-01	CM-01	CM-01		CM-01
CM	CM-02	CM-2	Baseline Configuration	a. Develop, document, and maintain under configuration control, a current baseline configuration of the system; and b. Review and update the baseline configuration of the system: 1. [Assignment: organization-defined frequency]; 2. When required due to [Assignment: organization-defined circumstances]; and 3. When system components are installed or upgraded.	CM-2	Low	Functional	Intersects With	5	Reviews & Updates	CFG-02.1	(1) At least annually; (2) When required due to so; or (3) As part of change management process.	CM-2	CM-2	CM-2	CM-2	CM-02	CM-02	CM-02	CM-02	CM-2	CM-2	CM-2	CM-2	CM-2	CM-02	CM-02	CM-02	CM-02	CM-02
CM	CM-02	CM-2	Baseline Configuration	a. Develop, document, and maintain under configuration control, a current baseline configuration of the system; and b. Review and update the baseline configuration of the system: 1. [Assignment: organization-defined frequency]; 2. When required due to [Assignment: organization-defined circumstances]; and 3. When system components are installed or upgraded.	CM-2	Low	Functional	Intersects With	5	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	CM-2	CM-2	CM-2		CM-02	CM-02	CM-02	CM-02	CM-2	CM-2	CM-2	CM-2	CM-2	CM-02	CM-02	CM-02	CM-02	CM-02
CM	CM-02(01)	CM-2(1)		Withdrawn	CM-2(1)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																CM-02(01)	CM-02(01)			CM-02(01)
CM	CM-02(02)	CM-2(2)	Baseline Configuration | Automation Support for Accuracy and Currency	Maintain the currency, completeness, accuracy, and availability of the baseline configuration of the system using [Assignment: organization-defined automated mechanisms].	CM-2(2)	Moderate	Functional	Equal	10	Automated Central Management & Verification	CFG-02.2	Automated mechanisms exist to govern and report on baseline configurations of Technology Assets, Applications and/or Services (TAAS) through Continuous Diagnostics and Mitigation (CDM), or similar technologies.		CM-2(2)	CM-2(2)			CM-02(02)	CM-02(02)									CM-02(02)	CM-02(02)	CM-02(02)
CM	CM-02(03)	CM-2(3)	Baseline Configuration | Retention of Previous Configurations	Retain [Assignment: organization-defined number] of previous versions of baseline configurations of the system.	CM-2(3)	Moderate	Functional	Equal	10	Retention Of Previous Configurations	CFG-02.3	Mechanisms exist to retain previous versions of baseline configuration to support roll back.		CM-2(3)	CM-2(3)			CM-02(03)	CM-02(03)								CM-02(03)	CM-02(03)		CM-02(03)
CM	CM-02(04)	CM-2(4)		Withdrawn	CM-2(4)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																			
CM	CM-02(05)	CM-2(5)		Withdrawn	CM-2(5)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																			
CM	CM-02(06)	CM-2(6)	Baseline Configuration | Development and Test Environments	Maintain a baseline configuration for system development and test environments that is managed separately from the operational baseline configuration.	CM-2(6)	Not Selected	Functional	Equal	10	Development & Test Environment Configurations	CFG-02.4	Mechanisms exist to manage baseline configurations for development and test environments separately from operational baseline configurations to minimize the risk of unintentional changes.											CM-2(6)	CM-2(6)							
CM	CM-02(07)	CM-2(7)	Baseline Configuration | Configure Systems and Components for High-risk Areas	a. Issue [Assignment: organization-defined configurations] to individuals traveling to locations that the organization deems to be of significant risk; and b. Apply [Assignment: organization-defined controls] to the systems or components when the individuals return from travel.	CM-2(7)	Moderate	Functional	Equal	10	Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.			CM-2(7)	CM-2(7)			CM-02(07)	CM-02(07)									CM-02(07)		CM-02(07)
CM	CM-03	CM-3	Configuration Change Control	a. Determine and document the types of changes to the system that are configuration-controlled; b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses; c. Document configuration change decisions associated with the system; d. Implement approved configuration-controlled changes to the system; e. Retain records of configuration-controlled changes to the system for [Assignment: organization-defined time period]; f. Monitor and review activities associated with configuration-controlled changes to the system; and g. Coordinate and provide oversight for configuration change control activities through [Assignment: organization-defined configuration change control element (e.g., committee, board)] that convenes [Selection (one or more): [Assignment: organization-defined frequency]; when [Assignment: organization-defined configuration changes]].	CM-3	Moderate	Functional	Subset Of	10	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	CM-3	CM-3	CM-3	CM-3	CM-03	CM-03	CM-03	CM-03	CM-3	CM-3	CM-3	CM-3	CM-3	CM-03	CM-03		CM-03
CM	CM-03	CM-3	Configuration Change Control	a. Determine and document the types of changes to the system that are configuration-controlled; b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses; c. Document configuration change decisions associated with the system; d. Implement approved configuration-controlled changes to the system; e. Retain records of configuration-controlled changes to the system for [Assignment: organization-defined time period]; f. Monitor and review activities associated with configuration-controlled changes to the system; and g. Coordinate and provide oversight for configuration change control activities through [Assignment: organization-defined configuration change control element (e.g., committee, board)] that convenes [Selection (one or more): [Assignment: organization-defined frequency]; when [Assignment: organization-defined configuration changes]].	CM-3	Moderate	Functional	Intersects With	5	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	CM-3	CM-3	CM-3	CM-3	CM-03	CM-03	CM-03	CM-03	CM-3	CM-3	CM-3	CM-3	CM-3	CM-03	CM-03		CM-03
CM	CM-03(01)	CM-3(1)	Configuration Change Control | Automated Documentation, Notification, and Prohibition of Changes	Use [Assignment: organization-defined automated mechanisms] to: (a) Document proposed changes to the system; (b) Notify [Assignment: organization-defined approval authorities] of proposed changes to the system and request change approval; (c) Highlight proposed changes to the system that have not been approved or disapproved within [Assignment: organization-defined time period]; (d) Prohibit changes to the system until designated approvals are received; (e) Document all changes to the system; and (f) Notify [Assignment: organization-defined personnel or roles] when approved changes to the system are completed.	CM-3(1)	High	Functional	Equal	10	Prohibition Of Changes	CHG-02.1	Mechanisms exist to prohibit unauthorized changes, unless organization-approved change requests are received.				CM-3(1)				CM-03(01)					CM-3(1)	CM-3(1)			CM-03(01)
CM	CM-03(02)	CM-3(2)	Configuration Change Control | Testing, Validation, and Documentation of Changes	Test, validate, and document changes to the system before finalizing the implementation of the changes.	CM-3(2)	Moderate	Functional	Intersects With	5	Control Functionality Verification	CHG-06	Mechanisms exist to verify the functionality of cybersecurity and/or data privacy controls following implemented changes to ensure applicable controls operate as designed.	CM-3(2)	CM-3(2)	CM-3(2)	CM-3(2)	CM-03(02)	CM-03(02)	CM-03(02)	CM-03(02)	CM-3(2)	CM-3(2)	CM-3(2)	CM-3(2)	CM-3(2)	CM-03(02)	CM-03(02)	CM-03(02)		CM-03(02)
CM	CM-03(02)	CM-3(2)	Configuration Change Control | Testing, Validation, and Documentation of Changes	Test, validate, and document changes to the system before finalizing the implementation of the changes.	CM-3(2)	Moderate	Functional	Intersects With	5	Test, Validate & Document Changes	CHG-02.2	Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented in a production environment.	CM-3(2)	CM-3(2)	CM-3(2)	CM-3(2)	CM-03(02)	CM-03(02)	CM-03(02)	CM-03(02)	CM-3(2)	CM-3(2)	CM-3(2)	CM-3(2)	CM-3(2)	CM-03(02)	CM-03(02)	CM-03(02)		CM-03(02)
CM	CM-03(03)	CM-3(3)	Configuration Change Control | Automated Change Implementation	Implement changes to the current system baseline and deploy the updated baseline across the installed base using [Assignment: organization-defined automated mechanisms].	CM-3(3)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																			
CM	CM-03(04)	CM-3(4)	Configuration Change Control | Security and Privacy Representatives	Require [Assignment: organization-defined security and privacy representatives] to be members of the [Assignment: organization-defined configuration change control element].	CM-3(4)	Moderate	Functional	Equal	10	Cybersecurity & Data Protection Representative for Asset Lifecycle Changes	CHG-02.3	Mechanisms exist to include a cybersecurity and/or data protection representative in the configuration change control review process.		CM-3(4)	CM-3(4)			CM-03(04)	CM-03(04)				CM-3(4)	CM-3(4)							CM-03(04)
CM	CM-03(05)	CM-3(5)	Configuration Change Control | Automated Security Response	Implement the following security responses automatically if baseline configurations are changed in an unauthorized manner: [Assignment: organization-defined security responses].	CM-3(5)	Not Selected	Functional	Equal	10	Automated Security Response	CHG-02.4	Automated mechanisms exist to implement remediation actions upon the detection of unauthorized baseline configurations change(s).																			
CM	CM-03(06)	CM-3(6)	Configuration Change Control | Cryptography Management	Ensure that the following controls are under configuration management: [Assignment: organization-defined security and privacy controls].	CM-3(6)	High	Functional	Equal	10	Cryptographic Management	CHG-02.5	Mechanisms exist to govern assets involved in providing cryptographic protections according to the organization's cryptographic management processes.			CM-3(6)				CM-03(06)												CM-03(06)
CM	CM-03(07)	CM-3(7)	Configuration Change Control | Review System Changes	Review changes to the system [Assignment: organization-defined frequency] or when [Assignment: organization-defined circumstances] to determine whether unauthorized changes have occurred.	CM-3(7)	Not Selected	Functional	Intersects With	5	Test, Validate & Document Changes	CHG-02.2	Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented in a production environment.																			
CM	CM-03(08)	CM-3(8)	Configuration Change Control | Prevent or Restrict Configuration Changes	Prevent or restrict changes to the configuration of the system under the following circumstances: [Assignment: organization-defined circumstances].	CM-3(8)	Not Selected	Functional	Equal	10	Configuration Enforcement	CFG-06	Automated mechanisms exist to monitor, enforce and report on configurations for endpoint devices.											CM-3(8)	CM-3(8)							
CM	CM-03(08)	CM-3(8)	Configuration Change Control | Prevent or Restrict Configuration Changes	Prevent or restrict changes to the configuration of the system under the following circumstances: [Assignment: organization-defined circumstances].	CM-3(8)	Not Selected	Functional	Intersects With	5	Integrity Assurance & Enforcement (IAE)	CFG-06.1	Automated mechanisms exist to identify unauthorized deviations from an approved baseline and implement automated resiliency actions to remediate the unauthorized change.											CM-3(8)	CM-3(8)							
CM	CM-04	CM-4	Impact Analyses	Analyze changes to the system, environment of operation, or environment of use in accordance with the following analysis methods: [Assignment: organization-defined analysis methods].	CM-4	Low	Functional	Equal	10	Security Impact Analysis for Changes	CHG-03	Mechanisms exist to analyze proposed changes for potential security impacts, prior to the implementation of the change.	CM-4	CM-4	CM-4	CM-4	CM-04	CM-04	CM-04	CM-04	CM-4				CM-4	CM-04	CM-04	CM-04	CM-04	CM-04
CM	CM-04(01)	CM-4(1)	Impact Analyses | Separate Test Environments	Analyze changes to the system in a separate test environment before implementation in an operational environment, looking for security and privacy impacts due to flaws, weaknesses, incompatibility, or intentional malice.	CM-4(1)	High	Functional	Equal	10	Separation of Development, Testing and Operational Environments	TDA-08	Mechanisms exist to manage separate development, testing and operational environments to reduce the risks of unauthorized access or changes to the operational environment and to ensure no impact to production Technology Assets, Applications and/or Services (TAAS).							CM-04(01)	CM-04(01)				CM-4(1)							CM-04(01)
CM	CM-04(02)	CM-4(2)	Impact Analyses | Verification of Controls	After the implementation of changes to the system, verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security and privacy requirements for the system.	CM-4(2)	Moderate	Functional	Equal	10	Technical Verification	IAO-06	Mechanisms exist to perform Information Assurance Program (IAP) activities to evaluate the design, implementation and effectiveness of technical cybersecurity and data protection controls.		CM-4(2)	CM-4(2)			CM-04(02)	CM-04(02)											
CM	CM-05	CM-5	Access Restrictions for Change	Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.	CM-5	Low	Functional	Intersects With	5	Governing Access Restriction for Change	END-03.2	Mechanisms exist to define, document, approve and enforce access restrictions associated with changes to Technology Assets, Applications and/or Services (TAAS).	CM-5	CM-5	CM-5	CM-5	CM-05	CM-05	CM-05	CM-05	CM-5	CM-5	CM-5	CM-5	CM-5	CM-05	CM-05	CM-05	CM-05	CM-05
CM	CM-05	CM-5	Access Restrictions for Change	Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.	CM-5	Low	Functional	Intersects With	5	Access Restriction For Change	CHG-04	Mechanisms exist to enforce configuration restrictions in an effort to restrict the ability of users to conduct unauthorized changes.	CM-5	CM-5	CM-5	CM-5	CM-05	CM-05	CM-05	CM-05	CM-5	CM-5	CM-5	CM-5	CM-5	CM-05	CM-05	CM-05	CM-05	CM-05
CM	CM-05(01)	CM-5(1)	Access Restrictions for Change | Automated Access Enforcement and Audit Records	Enforce access restrictions using [Assignment: organization-defined automated mechanisms]; and b. Automatically generate audit records of the enforcement actions.	CM-5(1)	High	Functional	Equal	10	Automated Access Enforcement / Auditing	CHG-04.1	Mechanisms exist to perform after-the-fact reviews of configuration change logs to discover any unauthorized changes.						CM-05(01)	CM-05(01)				CM-5(1)				CM-05(01)	CM-05(01)	CM-05(01)	CM-05(01)	
CM	CM-05(02)	CM-5(2)		Withdrawn	CM-5(2)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																			
CM	CM-05(03)	CM-5(3)		Withdrawn	CM-5(3)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																	CM-05(03)			
CM	CM-05(04)	CM-5(4)	Access Restrictions for Change | Dual Authorization	Enforce dual authorization for [Assignment: organization-defined system components or system-related information] within a production or operational environment; and b. Review and reevaluate dual authorization [Assignment: organization-defined frequency].	CM-5(4)	Not Selected	Functional	Equal	10	Dual Authorization for Change	CHG-04.3	Mechanisms exist to enforce a two-person rule for implementing changes to critical Technology Assets, Applications and/or Services (TAAS).																			
CM	CM-05(05)	CM-5(5)	Access Restrictions for Change | Privilege Limitation for Production and Operation	Limit privileges to change system components and system-related information within a production or operational environment; and b. Review and reevaluate privileges [Assignment: organization-defined frequency].	CM-5(5)	Not Selected	Functional	Equal	10	Permissions To Implement Changes	CHG-04.4	Mechanisms exist to limit operational privileges for implementing changes.						CM-05(05)	CM-05(05)								CM-05(05)	CM-05(05)	CM-05(05)	
CM	CM-05(06)	CM-5(6)	Access Restrictions for Change | Limit Library Privileges	Limit privileges to change software resident within software libraries.	CM-5(6)	Not Selected	Functional	Equal	10	Library Privileges	CHG-04.5	Mechanisms exist to restrict software library privileges to those individuals with a pertinent business need for access.											CM-5(6)							
CM	CM-05(07)	CM-5(7)		Withdrawn	CM-5(7)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																			
CM	CM-06	CM-6	Configuration Settings	a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using [Assignment: organization-defined common secure configurations]; b. Implement the configuration settings;c. Identify, document, and approve any deviations from established configuration settings for [Assignment: organization-defined system components] based on [Assignment: organization-defined operational requirements]; and d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.	CM-6	Low	Functional	Intersects With	5	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	CM-6	CM-6	CM-6	CM-6	CM-06	CM-06	CM-06	CM-06	CM-6	CM-6	CM-6	CM-6	CM-6	CM-06	CM-06	CM-06	CM-06	CM-06
CM	CM-06	CM-6	Configuration Settings	a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using [Assignment: organization-defined common secure configurations]; b. Implement the configuration settings;c. Identify, document, and approve any deviations from established configuration settings for [Assignment: organization-defined system components] based on [Assignment: organization-defined operational requirements]; and d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.	CM-6	Low	Functional	Intersects With	5	Approved Configuration Deviations	CFG-02.7	Mechanisms exist to document, assess risk and approve or deny deviations to standardized configurations.	CM-6	CM-6	CM-6	CM-6	CM-06	CM-06	CM-06	CM-06	CM-6	CM-6	CM-6	CM-6	CM-6	CM-06	CM-06	CM-06	CM-06	CM-06
CM	CM-06(01)	CM-6(1)	Configuration Settings | Automated Management, Application, and Verification	Manage, apply, and verify configuration settings for [Assignment: organization-defined system components] using [Assignment: organization-defined automated mechanisms].	CM-6(1)	High	Functional	Intersects With	5	Automated Central Management & Verification	CFG-02.2	Automated mechanisms exist to govern and report on baseline configurations of Technology Assets, Applications and/or Services (TAAS) through Continuous Diagnostics and Mitigation (CDM), or similar technologies.						CM-06(01)	CM-06(01)				CM-6(1)				CM-06(01)	CM-06(01)	CM-06(01)	CM-06(01)	
CM	CM-06(02)	CM-6(2)	Configuration Settings | Respond to Unauthorized Changes	Configure the system to respond to unauthorized changes to [Assignment: organization-defined configuration settings].	CM-6(2)	High	Functional	Equal	10	Respond To Unauthorized Changes	CFG-02.8	Mechanisms exist to respond to unauthorized changes to configuration settings as security incidents.							CM-06(02)				CM-6(2)							CM-06(02)
CM	CM-06(03)	CM-6(3)		Withdrawn	CM-6(3)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																			
CM	CM-06(04)	CM-6(4)		Withdrawn	CM-6(4)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																			
CM	CM-07	CM-7	Least Functionality	a. Configure the system to provide only [Assignment: organization-defined mission essential capabilities]; and b. Prohibit or restrict the use of the following functions, ports, protocols, software, and/or services: [Assignment: organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services].	CM-7	Low	Functional	Equal	10	Least Functionality	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, software and/or services.	CM-7	CM-7	CM-7		CM-07	CM-07	CM-07	CM-07	CM-7	CM-7			CM-7	CM-07	CM-07	CM-07		CM-07
CM	CM-07(01)	CM-7(1)	Least Functionality | Periodic Review	a. Review the system [Assignment: organization-defined frequency] to identify unnecessary and/or nonsecure functions, ports, protocols, and services; and b. Disable the functions, ports, protocols, and services within the system deemed to be unnecessary and/or nonsecure.	CM-7(1)	Moderate	Functional	Equal	10	Periodic Review	CFG-03.1	Mechanisms exist to periodically review system configurations to identify and disable unnecessary and/or non-secure functions, ports, protocols and services.		CM-7(1)	CM-7(1)			CM-07(01)	CM-07(01)				CM-7(1)	CM-7(1)			CM-07(01)		CM-07(01)	
CM	CM-07(02)	CM-7(2)	Least Functionality | Prevent Program Execution	Prevent program execution in accordance with [Assignment: organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions]; and b. Rules authorizing the terms and conditions of software program usage.	CM-7(2)	Moderate	Functional	Intersects With	5	Prevent Program Execution	SEA-06	Automated mechanisms exist to prevent the execution of unauthorized software programs.	CM-7(2)	CM-7(2)	CM-7(2)	CM-7(2)	CM-07(02)	CM-07(02)	CM-07(02)	CM-07(02)	CM-7(2)	CM-7(2)	CM-7(2)	CM-7(2)	CM-7(2)	CM-07(02)	CM-07(02)	CM-07(02)		CM-07(02)
CM	CM-07(02)	CM-7(2)	Least Functionality | Prevent Program Execution	Prevent program execution in accordance with [Assignment: organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions]; and b. Rules authorizing the terms and conditions of software program usage.	CM-7(2)	Moderate	Functional	Intersects With	5	Prevent Unauthorized Software Execution	CFG-03.2	Mechanisms exist to configure systems to prevent the execution of unauthorized software programs.	CM-7(2)	CM-7(2)	CM-7(2)	CM-7(2)	CM-07(02)	CM-07(02)	CM-07(02)	CM-07(02)	CM-7(2)	CM-7(2)	CM-7(2)	CM-7(2)	CM-7(2)	CM-07(02)	CM-07(02)	CM-07(02)		CM-07(02)
CM	CM-07(03)	CM-7(3)	Least Functionality | Registration Compliance	Ensure that the following functions, ports, protocols, and services are registered before use within the system: [Assignment: organization-defined registration requirements for functions, ports, protocols, and services].	CM-7(3)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																			
CM	CM-07(04)	CM-7(4)	Least Functionality | Unauthorized Software — Deny-by-exception	[Withdrawn: Incorporated into CM-7(5).]	CM-7(4)	Not Selected	Functional	Equal	10	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.											CM-7(4)	CM-7(4)							
CM	CM-07(05)	CM-7(5)	Least Functionality | Authorized Software — Allow-by-exception	Identify [Assignment: organization-defined software programs authorized to execute on the system];	CM-7(5)	Moderate	Functional	Equal	10	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.		CM-7(5)	CM-7(5)			CM-07(05)	CM-07(05)				CM-7(5)				CM-07(05)		CM-07(05)	
CM	CM-07(06)	CM-7(6)	Least Functionality | Confined Environments with Limited Privileges	Require that the following user-installed software execute in a confined physical or virtual machine environment with limited privileges: [Assignment: organization-defined user-installed software].	CM-7(6)	Not Selected	Functional	Intersects With	5	Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.											CM-7(6)	CM-7(6)							
CM	CM-07(07)	CM-7(7)	Least Functionality | Code Execution in Protected Environments	Allow execution of binary or machine-executable code only in confined physical or virtual machine environments and with the explicit approval of [Assignment: organization-defined personnel or roles] when such code is: [Assignment: organization-defined conditions].	CM-7(7)	Not Selected	Functional	Intersects With	5	Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.											CM-7(7)							
CM	CM-07(08)	CM-7(8)	Least Functionality | Binary or Machine Executable Code	(a) Prevent the use of binary or machine-executable code on [Assignment: organization-defined systems or system components] that do not: (1) Exist for the following purposes: [Assignment: organization-defined binary or machine-executable code]; and (2) Are executed without the provision of source code; and (b) Allow exceptions only for compelling mission or operational requirements and with the explicit approval of the authorizing official.	CM-7(8)	Not Selected	Functional	Equal	10	Binary or Machine-Executable Code	END-06.7	Mechanisms exist to prohibit the use of binary or machine-executable code from sources with limited or no warranty and without access to source code.											CM-7(8)	CM-7(8)						
CM	CM-07(09)	CM-7(9)	Least Functionality | Prohibiting The Use of Unauthorized Hardware	(a) Identify [Assignment: organization-defined hardware components] authorized for use by the system; (b) Prohibit the use or connection of unauthorized hardware components; (c) Review and update the list of authorized hardware components [Assignment: organization-defined frequency]; and (d) Disable unauthorized hardware components [Selection (one or more): detect; prevent; disable].	CM-7(9)	Not Selected	Functional	Intersects With	5	Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5

Family	Sorting Control #	Focal Document Element	Focal Document Element Name	Focal Document Element Description	NIST SP 800-53 R5.2	Security Control Baseline	Set Theory Relationship Mapping (STRM) Rationale	Relationship	Strength of Relationship	Reference Document Element	Reference Document Name	Reference Document Element Description	NIST SP 800-53 R5.2 Baselines Low	Mod	High	Privacy	FedRAMP R5 Low	Mod	High	LI-SaaS	CSCRM Baseline	NIST SP 800-161 R1 Down	Level 1	Level 2	Level 3	GovRAMP Low	Low+	Moderate	Core	High (FedRAMP Rev. 5)
CP	CP-02	CP-2	Contingency Plan	personnel (identified by name and/or by role) and organizational elements]c. Coordinate contingency	CP-2	Low	Functional	Intersects With	5	Ongoing Contingency Planning	BCD-06	Mechanisms exist to keep contingency plans current with business needs, technology changes and feedback from contingency plan testing activities.	CP-2	CP-2	CP-2	CP-2	CP-02	CP-02	CP-02	CP-02	CP-2	CP-2	CP-2	CP-2	CP-2	CP-02	CP-02	CP-02		CP-02
CP	CP-02(01)	CP-2(1)	Contingency Plan | Coordinate with Related Plans	Coordinate contingency plan development with organizational elements responsible for related plans.	CP-2(1)	Moderate	Functional	Equal	10	Coordinate with Related Plans	BCD-01.1	Mechanisms exist to coordinate contingency plan development with internal and external elements responsible for related plans.		CP-2(1)	CP-2(1)			CP-02(01)	CP-02(01)					CP-2(1)	CP-2(1)			CP-02(01)		CP-02(01)
CP	CP-02(02)	CP-2(2)	Contingency Plan | Capacity Planning	Conduct capacity planning so that necessary capacity for information processing, telecommunications and environmental support exist during contingency	CP-2(2)	High	Functional	Equal	10	Capacity Planning	CAP-03	Mechanisms exist to conduct capacity planning so that necessary capacity for information processing, telecommunications and environmental support will exist during contingency operations.			CP-2(2)				CP-02(02)						CP-2(2)	CP-2(2)			CP-02(02)		CP-02(02)
CP	CP-02(03)	CP-2(3)	Contingency Plan | Resume Mission and Business Functions	Plan for resumption of [Selection (one or more): all; essential] mission and business functions	CP-2(3)	Moderate	Functional	Intersects With	5	Resume All Missions & Business Functions	BCD-02.1	Mechanisms exist to resume all missions and business functions within Recovery Time Objectives (RTOs) of the contingency plan's activation.	CP-2(3)	CP-2(3)	CP-2(3)	CP-2(3)	CP-02(03)	CP-02(03)	CP-02(03)	CP-02(03)	CP-2(3)	CP-2(3)	CP-2(3)	CP-2(3)	CP-2(3)			CP-02(03)		CP-02(03)
CP	CP-02(03)	CP-2(3)	Contingency Plan | Resume Mission and Business Functions	Plan for resumption of [Selection (one): all; essential] mission and business functions within [Assignment: organization-defined time period] of contingency plan	CP-2(3)	Moderate	Functional	Intersects With	5	Resume Essential Missions & Business Functions	BCD-02.3	Mechanisms exist to resume essential missions and business functions within an organization-defined time period of contingency plan activation.	CP-2(3)	CP-2(3)	CP-2(3)	CP-2(3)	CP-02(03)	CP-02(03)	CP-02(03)	CP-02(03)	CP-2(3)	CP-2(3)	CP-2(3)	CP-2(3)	CP-2(3)			CP-02(03)		CP-02(03)
CP	CP-02(04)	CP-2(4)		Withdrawn	CP-2(4)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		CP-02(04)
CP	CP-02(05)	CP-2(5)	Contingency Plan | Continue Mission and Business Functions	Plan for continuation of [Selection (one): all; essential] mission and business functions with minimal or no loss of operational continuity and sustains that	CP-2(5)	High	Functional	Equal	10	Continue Essential Mission & Business Functions	BCD-02.2	Mechanisms exist to continue essential missions and business functions with little or no loss of operational continuity and sustain that continuity until full system restoration at primary processing			CP-2(5)				CP-02(05)											CP-02(05)
CP	CP-02(06)	CP-2(6)	Contingency Plan | Alternate Processing and Storage Sites	Plan for the transfer of [Assignment: organization-defined mission and business functions] to alternate processing and/or storage sites with minimal or no loss of operational continuity and sustain that continuity	CP-2(6)	Not Selected	Functional	Equal	10	Transfer to Alternate Processing / Storage Site	BCD-01.3	Mechanisms exist to redeploy personnel to other roles during a disruptive event or in the execution of a contingency plan.																		
CP	CP-02(07)	CP-2(7)	Contingency Plan | Coordinate with External Service Providers	Coordinate the contingency plan with the contingency plans of external service providers to ensure that	CP-2(7)	Not Selected	Functional	Equal	10	Coordinate With External Service Providers	BCD-01.2	Mechanisms exist to coordinate internal contingency plans with the contingency plans of external service providers to ensure that contingency requirements can be satisfied.									CP-2(7)			CP-2(7)						
CP	CP-02(08)	CP-2(8)	Contingency Plan | Identify Critical Assets	Identify critical system assets supporting [Selection (one): all; essential] mission and business functions.	CP-2(8)	Moderate	Functional	Equal	10	Identify Critical Assets	BCD-02	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TASD) that support essential missions and business functions.		CP-2(8)	CP-2(8)			CP-02(08)	CP-02(08)						CP-2(8)			CP-02(08)	CP-02(08)	CP-02(08)
CP	CP-03	CP-3	Contingency Training	Provide contingency training to system users consistent with assigned roles and responsibilities:	CP-3	Low	Functional	Equal	10	Contingency Training	BCD-03	Mechanisms exist to adequately train contingency personnel and applicable stakeholders in their contingency roles and responsibilities.	CP-3	CP-3	CP-3		CP-03	CP-03	CP-03	CP-03	CP-3	CP-3		CP-3	CP-3	CP-03	CP-03	CP-03		CP-03
CP	CP-03(01)	CP-3(1)	Contingency Training | Simulated Events	Incorporate simulated events into contingency training to facilitate effective response by personnel in crisis	CP-3(1)	High	Functional	Equal	10	Simulated Events	BCD-03.1	Mechanisms exist to incorporate simulated events into contingency training to facilitate effective response by personnel in crisis situations.			CP-3(1)				CP-03(01)					CP-3(1)	CP-3(1)			CP-03(01)		CP-03(01)
CP	CP-03(02)	CP-3(2)	Contingency Training | Mechanisms Used in Training Environments	Employ mechanisms used in operations to provide a more thorough and realistic contingency training	CP-3(2)	Not Selected	Functional	Equal	10	Automated Training Environments	BCD-03.2	Automated mechanisms exist to provide a more thorough and realistic contingency training environment.																		
CP	CP-04	CP-4	Contingency Plan Testing	Test the contingency plan for the system [Assignment: organization-defined frequency] using [Assignment: organization-defined tests] to determine the plan	CP-4	Low	Functional	Intersects With	5	Contingency Plan Root Cause Analysis (RCA) & Lessons Learned	BCD-05	Mechanisms exist to conduct a Root Cause Analysis (RCA) and "lessons learned" activity every time the contingency plan is activated.	CP-4	CP-4	CP-4	CP-4	CP-04	CP-04	CP-04	CP-04	CP-4	CP-4	CP-4	CP-4	CP-4	CP-04	CP-04	CP-04		CP-04
CP	CP-04	CP-4	Contingency Plan Testing	Test the contingency plan for the system [Assignment: organization-defined frequency] using [Assignment: organization-defined tests] to determine the plan	CP-4	Low	Functional	Intersects With	5	Contingency Plan Testing & Exercises	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	CP-4	CP-4	CP-4	CP-4	CP-04	CP-04	CP-04	CP-04	CP-4	CP-4	CP-4	CP-4	CP-4	CP-04	CP-04	CP-04		CP-04
CP	CP-04(01)	CP-4(1)	Contingency Plan Testing | Coordinate with Related Plans	Coordinate contingency plan testing with organizational elements responsible for related plans.	CP-4(1)	Moderate	Functional	Equal	10	Coordinated Testing with Related Plans	BCD-04.1	Mechanisms exist to coordinate contingency plan testing with internal and external elements responsible for related plans.			CP-4(1)	CP-4(1)			CP-04(01)	CP-04(01)									CP-04(01)		CP-04(01)
CP	CP-04(02)	CP-4(2)	Contingency Plan Testing | Alternate Processing Site	Test the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources; and	CP-4(2)	High	Functional	Equal	10	Alternate Storage & Processing Sites	BCD-04.2	Mechanisms exist to conduct contingency plan testing at alternate processing sites to both familiarize contingency personnel with the facility and evaluate the capabilities of the alternate processing site to			CP-4(2)				CP-04(02)											CP-04(02)
CP	CP-04(03)	CP-4(3)	Contingency Plan Testing | Automated Testing	Test the contingency plan using [Assignment: organization-defined automated mechanisms].	CP-4(3)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
CP	CP-04(04)	CP-4(4)	Contingency Plan Testing | Full Recovery and Reconstitution	Include a full recovery and reconstitution of the system to a known state as part of contingency plan testing.	CP-4(4)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
CP	CP-04(05)	CP-4(5)	Contingency Plan Testing | Self-challenge	Employ [Assignment: organization-defined mechanisms] to [Assignment: organization-defined system or system component] to disrupt and adversely affect the system	CP-4(5)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
CP	CP-05	CP-5		Withdrawn	CP-5	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
CP	CP-06	CP-6	Alternate Storage Site	Establish an alternate storage site [Selection (one): co-located; not co-located] that includes both the assets and necessary	CP-6	Moderate	Functional	Equal	10	Alternate Storage Site	BCD-08	Mechanisms exist to establish an alternate storage site that includes both the assets and necessary agreements to permit the storage and recovery of system backup information.		CP-6	CP-6			CP-06	CP-06					CP-6	CP-6			CP-06	CP-06	CP-06
CP	CP-06(01)	CP-6(1)	Alternate Storage Site | Separation from Primary Site	Identify an alternate storage site that is separated from the primary storage site to reduce	CP-6(1)	Moderate	Functional	Equal	10	Separation from Primary Site	BCD-08.1	Mechanisms exist to separate the alternate storage site from the primary storage site to reduce susceptibility to similar threats.		CP-6(1)	CP-6(1)			CP-06(01)	CP-06(01)					CP-6(1)	CP-6(1)			CP-06(01)		CP-06(01)
CP	CP-06(02)	CP-6(2)	Alternate Storage Site | Recovery Time and Recovery Operations	Configure the alternate storage site to facilitate recovery operations in accordance with recovery time and	CP-6(2)	High	Functional	Intersects With	5	Recovery Time / Point Objectives (RTO / RPO)	BCD-01.4	Mechanisms exist to facilitate recovery operations in accordance with Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).			CP-6(2)				CP-06(02)											CP-06(02)
CP	CP-06(03)	CP-6(3)	Alternate Storage Site | Accessibility	Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or	CP-6(3)	Moderate	Functional	Equal	10	Accessibility	BCD-08.2	Mechanisms exist to identify and mitigate potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster.		CP-6(3)	CP-6(3)			CP-06(03)	CP-06(03)									CP-06(03)		CP-06(03)
CP	CP-07	CP-7	Alternate Processing Site	Establish an alternate processing site that provides security measures equivalent to that of the primary site	CP-7	Moderate	Functional	Equal	10	Alternate Processing Site	BCD-09	Mechanisms exist to establish an alternate processing site that provides security measures equivalent to that of the primary site.		CP-7	CP-7			CP-07	CP-07					CP-7	CP-7			CP-07	CP-07	CP-07	CP-07
CP	CP-07(01)	CP-7(1)	Alternate Processing Site | Separation from Primary Site	Identify an alternate processing site that is separated from the primary processing site to reduce	CP-7(1)	Moderate	Functional	Equal	10	Separation from Primary Site	BCD-09.1	Mechanisms exist to separate the alternate processing site from the primary processing site to reduce susceptibility to similar threats.		CP-7(1)	CP-7(1)			CP-07(01)	CP-07(01)									CP-07(01)		CP-07(01)
CP	CP-07(02)	CP-7(2)	Alternate Processing Site | Accessibility	Identify potential accessibility problems to the alternate processing site in the event of an area-wide disruption	CP-7(2)	Moderate	Functional	Equal	10	Accessibility	BCD-09.2	Mechanisms exist to identify and mitigate potential accessibility problems to the alternate processing site and possible mitigation actions, in the event of an area-wide disruption or disaster.		CP-7(2)	CP-7(2)			CP-07(02)	CP-07(02)									CP-07(02)		CP-07(02)
CP	CP-07(03)	CP-7(3)	Alternate Processing Site | Priority of Service	Develop alternate processing site agreements that contain priority-of-service provisions in accordance with	CP-7(3)	Moderate	Functional	Equal	10	Alternate Site Priority of Service	BCD-09.3	Mechanisms exist to address priority-of-service provisions in alternate processing and storage sites that support availability requirements, including Recovery Time Objectives (RTOs).		CP-7(3)	CP-7(3)			CP-07(03)	CP-07(03)									CP-07(03)		CP-07(03)
CP	CP-07(04)	CP-7(4)	Alternate Processing Site | Preparation for Use	Prepare the alternate processing site so that the site can serve as the operational site supporting essential	CP-7(4)	High	Functional	Equal	10	Preparation for Use	BCD-09.4	Mechanisms exist to prepare the alternate processing alternate to support essential missions and business functions so that the alternate site is capable of being used as the primary site.			CP-7(4)				CP-07(04)											CP-07(04)
CP	CP-07(05)	CP-7(5)		Withdrawn	CP-7(5)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
CP	CP-07(06)	CP-7(6)	Alternate Processing Site | Inability to Return to Primary Site	Plan and prepare for circumstances that preclude returning to the primary processing site.	CP-7(6)	Not Selected	Functional	Equal	10	Inability to Return to Primary Site	BCD-09.5	Mechanisms exist to plan and prepare for both natural and manmade circumstances that preclude returning to the primary processing site.																		
CP	CP-08	CP-8	Telecommunications Services	Establish alternate telecommunications services for [Assignment: organization-defined essential mission and business functions within [Assignment: organization-defined time period]	CP-8	Moderate	Functional	Intersects With	5	Telecommunications Services Availability	BCD-10	Mechanisms exist to reduce the likelihood of a single point of failure with primary telecommunications services.		CP-8	CP-8			CP-08	CP-08					CP-8	CP-8			CP-08	CP-08	CP-08	CP-08
CP	CP-08(01)	CP-8(1)	Telecommunications Services | Priority of Service Provisions	Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time	CP-8(1)	Moderate	Functional	Equal	10	Telecommunications Priority of Service Provisions	BCD-10.1	Mechanisms exist to develop primary and alternate telecommunications service agreements that contain priority-of-service provisions that support availability requirements, including Recovery Time Objectives (RTOs).		CP-8(1)	CP-8(1)			CP-08(01)	CP-08(01)									CP-08(01)	CP-08(01)	CP-08(01)
CP	CP-08(02)	CP-8(2)	Telecommunications Services | Single Points of Failure	Obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with	CP-8(2)	Moderate	Functional	Intersects With	5	Telecommunications Services Availability	BCD-10	Mechanisms exist to reduce the likelihood of a single point of failure with primary telecommunications services.		CP-8(2)	CP-8(2)			CP-08(02)	CP-08(02)									CP-08(02)	CP-08(02)	CP-08(02)
CP	CP-08(03)	CP-8(3)	Telecommunications Services | Separation of Primary and Alternate Providers	Obtain alternate telecommunications services from providers that are separated from primary service	CP-8(3)	High	Functional	Equal	10	Separation of Primary / Alternate Providers	BCD-10.2	Mechanisms exist to obtain alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.			CP-8(3)				CP-08(03)					CP-8(3)	CP-8(3)					CP-08(03)
CP	CP-08(04)	CP-8(4)	Telecommunications Services | Provider Contingency Plan	Require primary and alternate telecommunications service providers to have contingency plans that meet	CP-8(4)	High	Functional	Equal	10	Provider Contingency Plan	BCD-10.3	Mechanisms exist to contractually require external service providers to have contingency plans that meet organizational contingency requirements.			CP-8(4)				CP-08(04)					CP-8(4)	CP-8(4)					CP-08(04)
CP	CP-08(05)	CP-8(5)	Telecommunications Services | Alternate Telecommunication Service Testing	Test alternate telecommunication services [Assignment: organization-defined frequency].	CP-8(5)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
CP	CP-09	CP-9	System Backup	Conduct backups of system-level information [Assignment: organization-defined frequency] consistent with recovery time and recovery point objectives]; c. Conduct backups	CP-9	Low	Functional	Intersects With	5	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives	CP-9	CP-9	CP-9		CP-09	CP-09	CP-09	CP-09						CP-09	CP-09	CP-09	CP-09	CP-09
CP	CP-09(01)	CP-9(1)	System Backup | Testing for Reliability and Integrity	Test backup information [Assignment: organization-defined frequency] to verify media reliability and	CP-9(1)	Moderate	Functional	Intersects With	5	Testing for Reliability & Integrity	BCD-11.1	Mechanisms exist to routinely test backups that verify the reliability of the backup process, as well as the integrity and availability of the data.		CP-9(1)	CP-9(1)			CP-09(01)	CP-09(01)								CP-09(01)	CP-09(01)			CP-09(01)
CP	CP-09(02)	CP-9(2)	System Backup | Test Restoration Using Sampling	Test restoration of backup information using sampling [Assignment: organization-defined frequency].	CP-9(2)	High	Functional	Equal	10	Test Restoration Using Sampling	BCD-11.5	Mechanisms exist to utilize sampling of available backups to test recovery capabilities as part of business continuity plan testing.			CP-9(2)				CP-09(02)											CP-09(02)
CP	CP-09(03)	CP-9(3)	System Backup | Separate Storage for Critical Information	Store backup copies of [Assignment: organization-defined critical system software and other security-related information] in a separate facility or in a fire	CP-9(3)	High	Functional	Equal	10	Separate Storage for Critical Information	BCD-11.2	Mechanisms exist to store backup copies of critical software and other security-related information in a separate facility or in a fire-rated container that is not collocated with the system being backed up.			CP-9(3)				CP-09(03)									CP-09(03)		CP-09(03)
CP	CP-09(04)	CP-9(4)		Withdrawn	CP-9(4)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
CP	CP-09(05)	CP-9(5)	System Backup | Transfer to Alternate Storage Site	Transfer system backup information to the alternate storage site [Assignment: organization-defined time period and transfer rate consistent with the recovery	CP-9(5)	High	Functional	Equal	10	Transfer to Alternate Storage Site	BCD-11.6	Mechanisms exist to transfer backup data to the alternate storage site at a rate that is capable of meeting both Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).			CP-9(5)				CP-09(05)											CP-09(05)
CP	CP-09(06)	CP-9(6)	System Backup | Redundant Secondary System	Conduct system backup by maintaining a redundant secondary system that is not collocated with the primary system and that can be activated without loss of	CP-9(6)	Not Selected	Functional	Equal	10	Redundant Secondary System	BCD-11.7	Mechanisms exist to maintain a failover capability, which is not collocated with the primary Technology Asset, Application and/or Service (TAAS), which can be activated with little-to-no loss of information or																		
CP	CP-09(07)	CP-9(7)	System Backup | Dual Authorization for Deletion or Destruction	Enforce dual authorization for the deletion or destruction of [Assignment: organization-defined backup	CP-9(7)	Not Selected	Functional	Equal	10	Dual Authorization For Backup Media Destruction	BCD-11.8	Mechanisms exist to implement and enforce dual authorization for the deletion or destruction of sensitive backup media and data.																		
CP	CP-09(08)	CP-9(8)	System Backup | Cryptographic Protection	Implement cryptographic mechanisms to prevent the unauthorized disclosure and modification of backup	CP-9(8)	Moderate	Functional	Equal	10	Cryptographic Protection	BCD-11.4	Mechanisms exist to prevent the unauthorized disclosure and/or modification of backup information.			CP-9(8)	CP-9(8)			CP-09(08)	CP-09(08)											
CP	CP-10	CP-10	System Recovery and Reconstitution	Provide for the recovery and reconstitution of the system to a known state within [Assignment: organization-defined time period consistent with recovery time and	CP-10	Low	Functional	Intersects With	5	Information System Recovery & Reconstitution	BCD-12	Mechanisms exist to ensure the secure recovery and reconstitution of Technology Assets, Applications and/or Services (TAAS) to a known state after a disruption, compromise or failure.	CP-10	CP-10	CP-10	CP-10	CP-10	CP-10	CP-10	CP-10	CP-10	CP-10	CP-10	CP-10	CP-10	CP-10	CP-10	CP-10	CP-10	CP-10
CP	CP-10	CP-10	System Recovery and Reconstitution	Provide for the recovery and reconstitution of the system to a known state within [Assignment: organization-defined time period consistent with recovery time and	CP-10	Low	Functional	Intersects With	5	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan	CP-10	CP-10	CP-10	CP-10	CP-10	CP-10	CP-10	CP-10	CP-10	CP-10	CP-10	CP-10	CP-10	CP-10	CP-10	CP-10	CP-10	CP-10
CP	CP-10	CP-10	System Recovery and Reconstitution	Provide for the recovery and reconstitution of the system to a known state within [Assignment: organization-defined time period consistent with recovery time and	CP-10	Low	Functional	Intersects With	5	Recovery Time / Point Objectives (RTO / RPO)	BCD-01.4	Mechanisms exist to facilitate recovery operations in accordance with Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	CP-10	CP-10	CP-10	CP-10	CP-10	CP-10	CP-10	CP-10	CP-10	CP-10	CP-10	CP-10	CP-10	CP-10	CP-10	CP-10	CP-10	CP-10
CP	CP-10(01)	CP-10(1)		Withdrawn	CP-10(1)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
CP	CP-10(02)	CP-10(2)	System Recovery and Reconstitution | Transaction Recovery	Implement transaction recovery for systems that are transaction-based.	CP-10(2)	Moderate	Functional	Equal	10	Transaction Recovery	BCD-12.1	Mechanisms exist to utilize specialized backup mechanisms that will allow transaction recovery for transaction-based Technology Assets, Applications and/or Services (TAAS) in accordance with Recovery		CP-10(2)	CP-10(2)			CP-10(02)	CP-10(02)								CP-10(02)	CP-10(02)			CP-10(02)
CP	CP-10(03)	CP-10(3)		Withdrawn	CP-10(3)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
CP	CP-10(04)	CP-10(4)	System Recovery and Reconstitution | Restore Within Time Period	Provide the capability to restore system components within [Assignment: organization-defined restoration time periods] from configuration-controlled and integrity-protected	CP-10(4)	High	Functional	Equal	10	Restore Within Time Period	BCD-12.4	Mechanisms exist to restore Technology Assets, Applications, Services and/or Data (TAASD) within organization-defined restoration time-periods from configuration-controlled and integrity-protected			CP-10(4)				CP-10(04)											CP-10(04)
CP	CP-10(05)	CP-10(5)		Withdrawn	CP-10(5)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
CP	CP-10(06)	CP-10(6)	System Recovery and Reconstitution | Component Protection	Protect system components used for recovery and reconstitution.	CP-10(6)	Not Selected	Functional	Equal	10	Backup & Restoration Hardware Protection	BCD-13	Mechanisms exist to protect backup and restoration hardware and software.																		
CP	CP-11	CP-11	Alternate Communications Protocols	Provide the capability to employ [Assignment: organization-defined alternative communications protocols] in support of maintaining continuity of	CP-11	Not Selected	Functional	Intersects With	5	Telecommunications Services Availability	BCD-10	Mechanisms exist to reduce the likelihood of a single point of failure with primary telecommunications services.											CP-11	CP-11							
CP	CP-12	CP-12	Safe Mode	When [Assignment: organization-defined conditions] are detected, enter a safe mode of operation with [Assignment: organization-defined restrictions of safe	CP-12	Not Selected	Functional	Intersects With	5	Fail Secure	SEA-07.2	Mechanisms exist to enable systems to fail to an organization-defined known-state for types of failures, preserving system state information in failure.																		
CP	CP-13	CP-13	Alternative Security Mechanisms	Employ [Assignment: organization-defined security functions] for the following alternative security mechanisms:	CP-13	Not Selected	Functional	Equal	10	Alternative Security Measures	BCD-07	Mechanisms exist to implement alternative or compensating controls to satisfy security functions when the primary means of implementing the security function is unavailable or compromised.																		
IA	IA-01	IA-1	Policy and Procedures	Develop, document, and maintain under configuration control, a current baseline configuration of the system; and	IA-1	Low	Functional	Intersects With	5	Cybersecurity & Data Protection	GOV-03	Mechanisms exist to review the cybersecurity & data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their	IA-1	IA-1	IA-1	IA-1	IA-01	IA-01	IA-01	IA-01	IA-1	IA-1	IA-1	IA-1	IA-1	IA-01	IA-01	IA-01	IA-01	IA-01
IA	IA-01	IA-1	Policy and Procedures	Develop, document, and maintain under configuration control, a current baseline configuration of the system; and	IA-1	Low	Functional	Subset Of	10	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	IA-1	IA-1	IA-1	IA-1	IA-01	IA-01	IA-01	IA-01	IA-1	IA-1	IA-1	IA-1	IA-1	IA-01	IA-01	IA-01		IA-01
IA	IA-01	IA-1	Policy and Procedures	Develop, document, and maintain under configuration control, a current baseline configuration of the system; and	IA-1	Low	Functional	Intersects With	5	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	IA-1	IA-1	IA-1	IA-1	IA-01	IA-01	IA-01	IA-01	IA-1	IA-1	IA-1	IA-1	IA-1	IA-01	IA-01	IA-01		IA-01
IA	IA-02	IA-2	Identification and Authentication (organizational Users)	Uniquely identify and authenticate organizational users and associate that unique identification with processes	IA-2	Low	Functional	Equal	10	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	IA-2	IA-2	IA-2		IA-02	IA-02	IA-02	IA-02	IA-2	IA-2	IA-2	IA-2	IA-2	IA-02	IA-02	IA-02	IA-02	IA-02
IA	IA-02(01)	IA-2(1)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts	Implement multi-factor authentication for access to privileged accounts.	IA-2(1)	Low	Functional	Intersects With	5	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network	IA-2(1)	IA-2(1)	IA-2(1)	IA-2(1)	IA-02(01)	IA-02(01)	IA-02(01)	IA-02(01)	IA-2(1)	IA-2(1)	IA-2(1)	IA-2(1)	IA-2(1)	IA-02(01)	IA-02(01)	IA-02(01)	IA-02(01)	IA-02(01)
IA	IA-02(01)	IA-2(1)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts	Implement multi-factor authentication for access to privileged accounts.	IA-2(1)	Low	Functional	Intersects With	5	Local Access to Privileged Accounts	IAC-06.3	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate local access for privileged accounts.	IA-2(1)	IA-2(1)	IA-2(1)	IA-2(1)	IA-02(01)	IA-02(01)	IA-02(01)	IA-02(01)	IA-2(1)	IA-2(1)	IA-2(1)	IA-2(1)	IA-2(1)	IA-02(01)	IA-02(01)	IA-02(01)	IA-02(01)	IA-02(01)
IA	IA-02(01)	IA-2(1)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts	Implement multi-factor authentication for access to privileged accounts.	IA-2(1)	Low	Functional	Intersects With	5	Information Assurance Enabled Products	TDA-02.2	IT products to those products that have been successfully evaluated against a National Information Assurance partnership (NIAP)-approved Protection Profile or the cryptographic module is FIPS-validated	IA-2(1)	IA-2(1)	IA-2(1)	IA-2(1)	IA-02(01)	IA-02(01)	IA-02(01)	IA-02(01)	IA-2(1)	IA-2(1)	IA-2(1)	IA-2(1)	IA-2(1)	IA-02(01)	IA-02(01)	IA-02(01)	IA-02(01)	IA-02(01)
IA	IA-02(01)	IA-2(1)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts	Implement multi-factor authentication for access to privileged accounts.	IA-2(1)	Low	Functional	Intersects With	5	Out-of-Band Multi-Factor Authentication	IAC-06.4	privileged accounts such that one of the factors is independently provided by a device separate from	IA-2(1)	IA-2(1)	IA-2(1)	IA-2(1)	IA-02(01)	IA-02(01)	IA-02(01)	IA-02(01)	IA-2(1)	IA-2(1)	IA-2(1)	IA-2(1)	IA-2(1)	IA-02(01)	IA-02(01)	IA-02(01)	IA-02(01)	IA-02(01)
IA	IA-02(01)	IA-2(1)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts	Implement multi-factor authentication for access to privileged accounts.	IA-2(1)	Low	Functional	Intersects With	5	Network Access to Privileged Accounts	IAC-06.1	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for privileged accounts.	IA-2(1)	IA-2(1)	IA-2(1)	IA-2(1)	IA-02(01)	IA-02(01)	IA-02(01)	IA-02(01)	IA-2(1)	IA-2(1)	IA-2(1)	IA-2(1)	IA-2(1)	IA-02(01)	IA-02(01)	IA-02(01)	IA-02(01)	IA-02(01)
IA	IA-02(01)	IA-2(1)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts	Implement multi-factor authentication for access to privileged accounts.	IA-2(1)	Low	Functional	Intersects With	5	Network Access to Non-Privileged Accounts	IAC-06.2	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for non-privileged accounts.	IA-2(1)	IA-2(1)	IA-2(1)	IA-2(1)	IA-02(01)	IA-02(01)	IA-02(01)	IA-02(01)	IA-2(1)	IA-2(1)	IA-2(1)	IA-2(1)	IA-2(1)	IA-02(01)	IA-02(01)	IA-02(01)	IA-02(01)	IA-02(01)
IA	IA-02(01)	IA-2(1)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts	Implement multi-factor authentication for access to privileged accounts.	IA-2(1)	Low	Functional	Intersects With	5	Hardware Token-Based Authentication	IAC-10.7	Automated mechanisms exist to ensure organization-defined token quality requirements are satisfied for hardware token-based authentication.	IA-2(1)	IA-2(1)	IA-2(1)	IA-2(1)	IA-02(01)	IA-02(01)	IA-02(01)	IA-02(01)	IA-2(1)	IA-2(1)	IA-2(1)	IA-2(1)	IA-2(1)	IA-02(01)	IA-02(01)	IA-02(01)	IA-02(01)	IA-02(01)
IA	IA-02(02)	IA-2(2)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Non-privileged Accounts	Implement multi-factor authentication for access to non-privileged accounts.	IA-2(2)	Low	Functional	Intersects With	5	Information Assurance Enabled Products	TDA-02.2	IT products to those products that have been successfully evaluated against a National Information Assurance partnership (NIAP)-approved Protection Profile or the cryptographic module is FIPS-validated	IA-2(2)	IA-2(2)	IA-2(2)	IA-2(2)	IA-02(02)	IA-02(02)	IA-02(02)	IA-02(02)	IA-2(2)	IA-2(2)	IA-2(2)	IA-2(2)	IA-2(2)				IA-02(02)	IA-02(02)
IA	IA-02(

Family	Sorting Control #	Focal Document Element	Focal Document Element Name	Focal Document Element Description	NIST SP 800-53 R5.2	Security Control Baseline	Set Theory Relationship Mapping (STRM)			Reference Document Element	Reference Document Name	Reference Document Element Description	NIST SP 800-53 R5.2 Baselines				FedRAMP R5				C-SCRM Baseline	NIST SP 800-161 R1				GovRAMP				
							Rationale	Relationship	Strength of Relationship				Low	Mod	High	Privacy	Low	Mod	High	LI-SaaS		Low Impact Software	Level 1	Level 2	Level 3	Low	Low+	Moderate	Core	High (FedRAMP 20x)
IA	IA-04(01)	IA-4(1)	Identifier Management | Prohibit Account Identifiers as Public Identifiers	Prohibit the use of system account identifiers that are the same as public identifiers for individual accounts.	IA-4(1)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
IA	IA-04(02)	IA-4(2)		Withdrawn	IA-4(2)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																	
IA	IA-04(03)	IA-4(3)		Withdrawn	IA-4(3)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																	
IA	IA-04(04)	IA-4(4)	Identifier Management | Identify User Status	Manage individual identifiers by uniquely identifying each individual as [Assignment: organization-defined characteristic identifying individual status].	IA-4(4)	Moderate	Functional	Intersects With	5	Authenticate, Authorize and Audit (AAA)	IAC-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	IA-4(4)	IA-4(4)	IA-4(4)	IA-4(4)	IA-04(04)	IA-04(04)	IA-04(04)	IA-04(04)	IA-4(4)	IA-4(4)	IA-4(4)	IA-4(4)	IA-4(4)			IA-04(04)	IA-04(04)	IA-04(04)
IA	IA-04(04)	IA-4(4)	Identifier Management | Identify User Status	Manage individual identifiers by uniquely identifying each individual as [Assignment: organization-defined characteristic identifying individual status].	IA-4(4)	Moderate	Functional	Intersects With	5	User Identity (ID) Management	IAC-09.1	Mechanisms exist to ensure proper user identification management for non-consumer users and administrators.	IA-4(4)	IA-4(4)	IA-4(4)	IA-4(4)	IA-04(04)	IA-04(04)	IA-04(04)	IA-04(04)	IA-4(4)	IA-4(4)	IA-4(4)	IA-4(4)	IA-4(4)			IA-04(04)	IA-04(04)	IA-04(04)
IA	IA-04(04)	IA-4(4)	Identifier Management | Identify User Status	Manage individual identifiers by uniquely identifying each individual as [Assignment: organization-defined characteristic identifying individual status].	IA-4(4)	Moderate	Functional	Intersects With	5	Identity User Status	IAC-09.2	Mechanisms exist to identify contractors and other third-party users through unique username characteristics.	IA-4(4)	IA-4(4)	IA-4(4)	IA-4(4)	IA-04(04)	IA-04(04)	IA-04(04)	IA-04(04)	IA-4(4)	IA-4(4)	IA-4(4)	IA-4(4)	IA-4(4)			IA-04(04)	IA-04(04)	IA-04(04)
IA	IA-04(05)	IA-4(5)	Identifier Management | Dynamic Management	Manage individual identifiers dynamically in accordance with [Assignment: organization-defined dynamic identifier policy].	IA-4(5)	Not Selected	Functional	Intersects With	5	Dynamic Management	IAC-09.3	Mechanisms exist to dynamically manage usernames and system identifiers.																	
IA	IA-04(06)	IA-4(6)	Identifier Management | Cross-organization Management	Coordinate with the following external organizations for cross-organization management of identifiers: [Assignment: organization-defined external organizations].	IA-4(6)	Not Selected	Functional	Equal	10	Cross-Organization Management	IAC-09.4	Mechanisms exist to coordinate username identifiers with external organizations for cross-organization management of identifiers.							IA-4(6)	IA-4(6)	IA-4(6)								
IA	IA-04(07)	IA-4(7)		Withdrawn	IA-4(7)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																	
IA	IA-04(08)	IA-4(8)	Identifier Management | Pairwise Pseudonymous Identifiers	Generate pairwise pseudonymous identifiers.	IA-4(8)	Not Selected	Functional	Equal	10	Pairwise Pseudonymous Identifiers (PPID)	IAC-09.6	Mechanisms exist to generate pairwise pseudonymous identifiers with no identifying information about a data subject to discourage activity tracking and profiling of the data subject.																	
IA	IA-04(09)	IA-4(9)	Identifier Management | Attribute Maintenance and Protection	Maintain the attributes for each uniquely identified individual, device, or service in [Assignment: organization-defined characteristics identifying individual status].	IA-4(9)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
IA	IA-05	IA-5	Authenticator Management	For password-based authentication: a. Changing default authenticators prior to first use; b. Changing or refreshing authenticators [Assignment: organization-defined time period by authenticator type] or when events occur such as account compromise or breach; c. Protecting authenticator content from unauthorized disclosure and modification; d. Requiring individuals to take specific measures to safeguard authenticators; e. Changing authenticators prior to delivery and installation; f. Implementing specific controls to protect authenticators during the initial authenticator distribution; g. Changing authenticators for group or role accounts when membership to those accounts changes; and h. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators.	IA-5	Low	Functional	Intersects With	5	Authenticator Management	IAC-10	Mechanisms exist to securely manage authenticators for users and devices.	IA-5	IA-5	IA-5	IA-5	IA-05	IA-05	IA-05	IA-05	IA-5	IA-5	IA-5	IA-5	IA-5					
IA	IA-05	IA-5	Authenticator Management	For password-based authentication: a. Changing default authenticators prior to first use; b. Changing or refreshing authenticators [Assignment: organization-defined time period by authenticator type] or when events occur such as account compromise or breach; c. Protecting authenticator content from unauthorized disclosure and modification; d. Requiring individuals to take specific measures to safeguard authenticators; e. Changing authenticators prior to delivery and installation; f. Implementing specific controls to protect authenticators during the initial authenticator distribution; g. Changing authenticators for group or role accounts when membership to those accounts changes; and h. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators.	IA-5	Low	Functional	Intersects With	5	Default Authenticators	IAC-10.8	Mechanisms exist to ensure default authenticators are changed as part of account creation or system installation.	IA-5	IA-5	IA-5	IA-5	IA-05	IA-05	IA-05	IA-05	IA-5	IA-5	IA-5	IA-5	IA-5	IA-05	IA-05	IA-05	IA-05	IA-05
IA	IA-05(01)	IA-5(1)	Authenticator Management | Password-based Authentication	For password-based authentication: a. Maintain a list of commitments for password-protected cryptographically-protected channels; b. Store passwords using an approved salted key derivation function, preferably using a keyed hash; c. Require immediate selection of a new password upon account recovery; d. Allow user selection of long passwords and passphrases, including spaces and all printable characters; e. Employ automated tools to assist the user in selecting strong password authenticators; and f. Select a new or randomly generated password authenticator upon account recovery.	IA-5(1)	Low	Functional	Intersects With	5	Automated Support For Password Strength	IAC-10.4	Automated mechanisms exist to determine if password authenticators are sufficiently strong enough to satisfy organization-defined password length and complexity requirements.	IA-5(1)	IA-5(1)	IA-5(1)	IA-5(1)	IA-05(01)	IA-05(01)	IA-05(01)	IA-05(01)	IA-5(1)	IA-5(1)	IA-5(1)	IA-5(1)	IA-5(1)	IA-05(01)	IA-05(01)	IA-05(01)	IA-05(01)	IA-05(01)
IA	IA-05(01)	IA-5(1)	Authenticator Management | Password-based Authentication	For password-based authentication: a. Maintain a list of commitments for password-protected cryptographically-protected channels; b. Store passwords using an approved salted key derivation function, preferably using a keyed hash; c. Require immediate selection of a new password upon account recovery; d. Allow user selection of long passwords and passphrases, including spaces and all printable characters; e. Employ automated tools to assist the user in selecting strong password authenticators; and f. Select a new or randomly generated password authenticator upon account recovery.	IA-5(1)	Low	Functional	Intersects With	5	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	IA-5(1)	IA-5(1)	IA-5(1)	IA-5(1)	IA-05(01)	IA-05(01)	IA-05(01)	IA-05(01)	IA-5(1)	IA-5(1)	IA-5(1)	IA-5(1)	IA-5(1)	IA-05(01)	IA-05(01)	IA-05(01)	IA-05(01)	IA-05(01)
IA	IA-05(01)	IA-5(1)	Authenticator Management | Password-based Authentication	For password-based authentication: a. Maintain a list of commitments for password-protected cryptographically-protected channels; b. Store passwords using an approved salted key derivation function, preferably using a keyed hash; c. Require immediate selection of a new password upon account recovery; d. Allow user selection of long passwords and passphrases, including spaces and all printable characters; e. Employ automated tools to assist the user in selecting strong password authenticators; and f. Select a new or randomly generated password authenticator upon account recovery.	IA-5(1)	Low	Functional	Intersects With	5	Authenticator Management	IAC-10	Mechanisms exist to securely manage authenticators for users and devices.	IA-5(1)	IA-5(1)	IA-5(1)	IA-5(1)	IA-05(01)	IA-05(01)	IA-05(01)	IA-05(01)	IA-5(1)	IA-5(1)	IA-5(1)	IA-5(1)	IA-5(1)	IA-05(01)	IA-05(01)	IA-05(01)	IA-05(01)	IA-05(01)
IA	IA-05(02)	IA-5(2)	Authenticator Management | Public Key-based Authentication	For public key-based authentication: a. Enforce authorized access to the corresponding private key; and b. Map the authenticated identity to the account of the individual or group; and c. When public key infrastructure (PKI) is used:1. Validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information for PKI-based authentication;	IA-5(2)	Moderate	Functional	Equal	10	PKI-Based Authentication	IAC-10.2	to an accepted trust anchor including checking certificate status information for PKI-based	IA-5(2)	IA-5(2)	IA-5(2)	IA-5(2)	IA-05(02)	IA-05(02)	IA-05(02)	IA-05(02)	IA-5(2)	IA-5(2)	IA-5(2)	IA-5(2)	IA-5(2)			IA-05(02)		IA-05(02)
IA	IA-05(03)	IA-5(3)		Withdrawn	IA-5(3)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																IA-05(03)		IA-05(03)
IA	IA-05(04)	IA-5(4)		Withdrawn	IA-5(4)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																IA-05(04)		IA-05(04)
IA	IA-05(05)	IA-5(5)	Authenticator Management | Change Authenticators Prior to Delivery	Require developers and installers of system components to provide unique authenticators or change default authenticators prior to delivery and installation.	IA-5(5)	Not Selected	Functional	Intersects With	5	Default Authenticators	IAC-10.8	Mechanisms exist to ensure default authenticators are changed as part of account creation or system installation.											IA-5(5)							
IA	IA-05(06)	IA-5(6)	Authenticator Management | Protection of Authenticators	Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access.	IA-5(6)	Moderate	Functional	Intersects With	5	User Responsibilities for Account Management	IAC-18	Mechanisms exist to compel users to follow accepted practices in the use of authentication mechanisms (e.g., passwords, passphrases, physical or logical security tokens, smart cards,	IA-5(6)	IA-5(6)	IA-5(6)	IA-5(6)	IA-05(06)	IA-05(06)	IA-05(06)	IA-05(06)	IA-5(6)	IA-5(6)	IA-5(6)	IA-5(6)	IA-5(6)					
IA	IA-05(06)	IA-5(6)	Authenticator Management | Protection of Authenticators	Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access.	IA-5(6)	Moderate	Functional	Intersects With	5	Protection of Authenticators	IAC-10.5	Mechanisms exist to protect authenticators commensurate with the sensitivity of the information to which use of the authenticator permits access.	IA-5(6)	IA-5(6)	IA-5(6)	IA-5(6)	IA-05(06)	IA-05(06)	IA-05(06)	IA-05(06)	IA-5(6)	IA-5(6)	IA-5(6)	IA-5(6)	IA-5(6)			IA-05(06)		IA-05(06)
IA	IA-05(07)	IA-5(7)	Authenticator Management | No Embedded Unencrypted Static Authenticators	Ensure that unencrypted static authenticators are not embedded in applications, scripts or stored on function keys.	IA-5(7)	Not Selected	Functional	Equal	10	No Embedded Unencrypted Static Authenticators	IAC-10.6	Mechanisms exist to ensure that unencrypted, static authenticators are not embedded in applications, scripts or stored on function keys.					IA-05(07)	IA-05(07)										IA-05(07)		IA-05(07)
IA	IA-05(08)	IA-5(8)	Authenticator Management | Multiple System Accounts	Implement [Assignment: organization-defined security controls] to manage the risk of compromise due to individuals having accounts on multiple systems.	IA-5(8)	Not Selected	Functional	Intersects With	5	Multiple Information System Accounts	IAC-10.9	Mechanisms exist to implement security safeguards to manage the risk of compromise due to individuals having accounts on multiple Technology Assets, Applications and/or Services (TAAS).	IA-5(8)	IA-5(8)	IA-5(8)	IA-5(8)	IA-05(08)	IA-05(08)	IA-05(08)	IA-05(08)	IA-5(8)	IA-5(8)	IA-5(8)	IA-5(8)	IA-5(8)					
IA	IA-05(08)	IA-5(8)	Authenticator Management | Multiple System Accounts	Implement [Assignment: organization-defined security controls] to manage the risk of compromise due to individuals having accounts on multiple systems.	IA-5(8)	Not Selected	Functional	Equal	10	Privileged Account Identifiers	IAC-09.5	Mechanisms exist to uniquely manage privileged accounts to identify the account as a privileged user or service.	IA-5(8)	IA-5(8)	IA-5(8)	IA-5(8)	IA-05(08)	IA-05(08)	IA-05(08)	IA-05(08)	IA-5(8)	IA-5(8)	IA-5(8)	IA-5(8)	IA-5(8)			IA-05(08)		
IA	IA-05(09)	IA-5(9)	Authenticator Management | Federated Credential Management	Use the following external organizations to federate credentials: [Assignment: organization-defined external organizations].	IA-5(9)	Not Selected	Functional	Equal	10	Federated Credential Management	IAC-13.2	Mechanisms exist to federate credentials to allow cross-organization authentication of individuals and devices.											IA-5(9)							
IA	IA-05(10)	IA-5(10)	Authenticator Management | Dynamic Credential Binding	Bind identities and authenticators dynamically using the following rules: [Assignment: organization-defined rules].	IA-5(10)	Not Selected	Functional	Intersects With	5	Dynamic Management	IAC-09.3	Mechanisms exist to dynamically manage usernames and system identifiers.																	
IA	IA-05(11)	IA-5(11)		Withdrawn	IA-5(11)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A														IA-05(11)	IA-05(11)	IA-05(11)		IA-05(11)
IA	IA-05(12)	IA-5(12)	Authenticator Management | Biometric Authentication Performance	For biometric-based authentication, employ mechanisms that satisfy the following biometric quality requirements [Assignment: organization-defined biometric quality requirements].	IA-5(12)	Not Selected	Functional	Equal	10	Biometric Authentication	IAC-10.12	Mechanisms exist to ensure biometric-based authentication satisfies organization-defined biometric quality requirements for false positives and false negatives.																	
IA	IA-05(13)	IA-5(13)	Authenticator Management | Expiration of Cached Authenticators	Prohibit the use of cached authenticators after [Assignment: organization-defined time period].	IA-5(13)	Not Selected	Functional	Equal	10	Expiration of Cached Authenticators	IAC-10.10	Automated mechanisms exist to prohibit the use of cached authenticators after organization-defined time period.							IA-05(13)											IA-05(13)
IA	IA-05(14)	IA-5(14)	Authenticator Management | Managing Content of PKI Trust Stores	Employ a trust store management mechanism for PKI certificates, keys, and other materials in trust stores installed across all platforms, including networks, operating systems, browsers, and applications.	IA-5(14)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
IA	IA-05(15)	IA-5(15)	Authenticator Management | GSA-approved Products and Services	Use only General Services Administration-approved products and services for identity, credential, and access management with approved PKI Certificate Policies.	IA-5(15)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
IA	IA-05(16)	IA-5(16)	Authenticator Management | In-person or Trusted External Party Authenticator Issuance	Require that the issuance of [Assignment: organization-defined types] of and initial authenticator content be conducted [Selection (one): in-person; by a trusted external party] before [Assignment: organization-defined time period] after account creation.	IA-5(16)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
IA	IA-05(17)	IA-5(17)	Authenticator Management | Presentation Attack Detection for Biometric Authenticators	Employ presentation attack detection mechanisms for biometric-based authentication.	IA-5(17)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
IA	IA-05(18)	IA-5(18)	Authenticator Management | Password Managers	(a) Protect the passwords using [Assignment: organization-defined password manager]; and (b) Generate and manage passwords; and (c) Protect the passwords using [Assignment: organization-defined controls].	IA-5(18)	Not Selected	Functional	Equal	10	Password Managers	IAC-10.11	Mechanisms exist to protect and store passwords via a password manager tool.																	
IA	IA-06	IA-6	Authentication Feedback	Obscure the feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.	IA-6	Low	Functional	Equal	10	Authenticator Feedback	IAC-11	Mechanisms exist to obscure the feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	IA-6	IA-6	IA-6		IA-06	IA-06	IA-06	IA-06						IA-06	IA-06	IA-06		IA-06
IA	IA-07	IA-7	Cryptographic Module Authentication	Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication.	IA-7	Low	Functional	Intersects With	5	Cryptographic Module Authentication	IAC-12	Mechanisms exist to ensure cryptographic modules adhere to applicable statutory, regulatory and contractual requirements for security strength.	IA-7	IA-7	IA-7	IA-7	IA-07	IA-07	IA-07	IA-07	IA-7	IA-7	IA-7	IA-7	IA-7	IA-07	IA-07	IA-07		IA-07
IA	IA-07	IA-7	Cryptographic Module Authentication	Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication.	IA-7	Low	Functional	Intersects With	5	Cryptographic Module Authentication	CRY-02	Automated mechanisms exist to enable systems to authenticate to a cryptographic module.	IA-7	IA-7	IA-7	IA-7	IA-07	IA-07	IA-07	IA-07	IA-7	IA-7	IA-7	IA-7	IA-7	IA-07	IA-07	IA-07		IA-07
IA	IA-08	IA-8	Identification and Authentication (non-organizational Users)	Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.	IA-8	Low	Functional	Equal	10	Identification & Authentication for Non-Organizational Users	IAC-03	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) third-party users and processes that provide services to the organization.	IA-8	IA-8	IA-8		IA-08	IA-08	IA-08	IA-08	IA-8		IA-8		IA-8			IA-08	IA-08	IA-08
IA	IA-08(01)	IA-8(1)	Identification and Authentication (non-organizational Users) | Acceptance of PIV Credentials from Other Agencies	Accept and electronically verify Personal Identity Verification-compliant credentials from other federal agencies.	IA-8(1)	Low	Functional	Equal	10	Acceptance of PIV Credentials from Other Organizations	IAC-03.1	Automated mechanisms exist to accept and electronically verify Personal Identity Verification (PIV) credentials from third-parties.	IA-8(1)	IA-8(1)	IA-8(1)		IA-08(01)	IA-08(01)	IA-08(01)	IA-08(01)										IA-08(01)
IA	IA-08(02)	IA-8(2)	Identification and Authentication (non-organizational Users) | Acceptance of External Authenticators	Accept only external authenticators that are NIST-compliant; and Document and maintain a list of accepted external authenticators.	IA-8(2)	Low	Functional	Equal	10	Acceptance of Third-Party Credentials	IAC-03.2	Automated mechanisms exist to accept Federal Identity, Credential and Access Management (FICAM)-approved third-party credentials.	IA-8(2)	IA-8(2)	IA-8(2)		IA-08(02)	IA-08(02)	IA-08(02)	IA-08(02)										IA-08(02)
IA	IA-08(03)	IA-8(3)		Withdrawn	IA-8(3)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																	IA-08(03)
IA	IA-08(04)	IA-8(4)	Identification and Authentication (non-organizational Users) | Use of Defined Profiles	Conform to the following profiles for identity management [Assignment: organization-defined identity management profiles].	IA-8(4)	Low	Functional	Equal	10	Use of FICAM-Issued Profiles	IAC-03.3	Mechanisms exist to conform systems to Federal Identity, Credential and Access Management (FICAM)-issued profiles.	IA-8(4)	IA-8(4)	IA-8(4)		IA-08(04)	IA-08(04)	IA-08(04)	IA-08(04)										IA-08(04)
IA	IA-08(05)	IA-8(5)	Identification and Authentication (non-organizational Users) | Acceptance of PIV-I Credentials	Accept and verify federated or PKI credentials that meet [Assignment: organization-defined policy].	IA-8(5)	Not Selected	Functional	Equal	10	Acceptance of PIV Credentials	IAC-02.3	Mechanisms exist to accept and electronically verify organizational Personal Identity Verification (PIV) credentials.																	
IA	IA-08(06)	IA-8(6)	Identification and Authentication (non-organizational Users) | Disassociability	Implement the following measures to disassociate user attributes or identifiers assertion relationships among individuals, credential service providers, and relying parties: [Assignment: organization-defined system services and applications].	IA-8(6)	Not Selected	Functional	Equal	10	Disassociability	IAC-03.4	Mechanisms exist to disassociate user attributes or credential assertion relationships among individuals, credential service providers and relying parties.																	
IA	IA-09	IA-9	Service Identification and Authentication	Uniquely identify and authenticate [Assignment: organization-defined system services and applications] before establishing communications with devices, users, or other services or applications.	IA-9	Not Selected	Functional	Equal	10	Third-Party Assets, Applications & Services	IAC-05	Mechanisms exist to identify and authenticate third-party Technology Assets, Applications and/or Services (TAAS).									IA-9		IA-9	IA-9						
IA	IA-09(01)	IA-9(1)		Withdrawn	IA-9(1)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																	
IA	IA-09(02)	IA-9(2)		Withdrawn	IA-9(2)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																	
IA	IA-10	IA-10	Adaptive Authentication	Require different authentication strategies and mechanisms based on [Assignment: organization-defined adaptive authentication techniques or mechanisms] under [Assignment: organization-defined circumstances or situations].	IA-10	Not Selected	Functional	Equal	10	Adaptive Identification & Authentication	IAC-13	Mechanisms exist to allow individuals to utilize alternative methods of authentication under specific circumstances or situations.																	
IA	IA-11	IA-11	Re-authentication	Require users to re-authenticate when [Assignment: organization-defined circumstances or situations requiring re-authentication].	IA-11	Low	Functional	Equal	10	Re-Authentication	IAC-14	Mechanisms exist to force users and devices to re-authenticate according to organization-defined circumstances that necessitate re-authentication.	IA-11	IA-11	IA-11		IA-11	IA-11	IA-11	IA-11										
IA	IA-12	IA-12	Identity Proofing	(a) Identity proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines; b. Resolve user identities to a unique individual; and c. Collect, validate, and verify identity evidence.	IA-12	Moderate	Functional	Equal	10	Identity Proofing (Identity Verification)	IAC-28	Mechanisms exist to verify the identity of a user before issuing authenticators or modifying access permissions.		IA-12	IA-12			IA-12	IA-12										
IA	IA-12(01)	IA-12(1)	Identity Proofing | Supervisor Authorization	Require that the registration process to receive an account for logical access includes supervisor or sponsor authorization.	IA-12(1)	Not Selected	Functional	Intersects With	5	Management Approval For New or Changed Accounts	IAC-28.1	Mechanisms exist to ensure management approvals are required for new accounts or changes in permissions to existing accounts.																	
IA	IA-12(02)	IA-12(2)	Identity Proofing | Identity Evidence	Require evidence of individual identification be presented to the registration authority.	IA-12(2)	Moderate	Functional	Equal	10	Identity Evidence	IAC-28.2	Mechanisms exist to require evidence of individual identification to be presented to the registration authority.		IA-12(2)	IA-12(2)			IA-12(02)	IA-12(02)										
IA	IA-12(03)	IA-12(3)	Identity Proofing | Identity Evidence Validation and Verification	Require that the presented identity evidence be validated and verified through [Assignment: organizational defined methods of validation and verification].	IA-12(3)	Moderate	Functional	Equal	10	Identity Evidence Validation & Verification	IAC-28.3	Mechanisms exist to require that the presented identity evidence be validated and verified through organizational-defined methods of validation and verification.		IA-12(3)	IA-12(3)			IA-12(03)	IA-12(03)										
IA	IA-12(04)	IA-12(4)	Identity Proofing | In-person Validation and Verification	In-person validation and verification of [Assignment: organization-defined identity evidence] is required.	IA-12(4)	High	Functional	Intersects With	5	User Provisioning & De-Provisioning	IAC-07	Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.	IA-12(4)	IA-12(4)	IA-12(4)	IA-12(4)	IA-12(04)	IA-12(04)	IA-12(04)	IA-12(04)	IA-12(4)	IA-12(4)	IA-12(4)	IA-12(4)	IA-12(4)					
IA	IA-12(04)	IA-12(4)	Identity Proofing | In-person Validation and Verification	In-person validation and verification of [Assignment: organization-defined identity evidence] is required.	IA-12(4)	High	Functional	Intersects With	5	In-Person or Trusted Third-Party Registration	IAC-10.3	Mechanisms exist to conduct in-person or trusted third-party identify verification before user accounts for third-parties are created.	IA-12(4)	IA-12(4)	IA-12(4)	IA-12(4)	IA-12(04)	IA-12(04)	IA-12(04)	IA-12(04)	IA-12(4)	IA-12(4)	IA-12(4)	IA-12(4)	IA-12(4)					
IA	IA-12(04)	IA-12(4)	Identity Proofing | In-person Validation and Verification	In-person validation and verification of [Assignment: organization-defined identity evidence] is required.	IA-12(4)	High	Functional	Intersects With	5	In-Person Validation & Verification	IAC-28.4	Mechanisms exist to require that the validation and verification of identity evidence be conducted in person before a designated registration authority.	IA-12(4)	IA-12(4)	IA-12(4)	IA-12(4)	IA-12(04)	IA-12(04)	IA-12(04)	IA-12(04)	IA-12(4)	IA-12(4)	IA-12(4)	IA-12(4)	IA-12(4)					
IA	IA-12(05)	IA-12(5)	Identity Proofing | Address Confirmation	Require that a notice of proofing be delivered through an out-of-band channel to verify the user's address (physical or digital) of record.	IA-12(5)	Moderate	Functional	Equal	10	Address Confirmation	IAC-28.5	Mechanisms exist to require that a notice of proofing be delivered through an out-of-band channel to verify the user's address (physical or digital).		IA-12(5)	IA-12(5)			IA-12(05)	IA-12(05)										
IA	IA-12(06)	IA-12(6)	Identity Proofing | Accept Externally-proofed Identities	Accept the user-provided identity proof [Assignment: organization-defined identity assurance level] from [Assignment: organization-defined external organizations].	IA-12(6)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
IA	IA-13	IA-13	Identity Providers and Authorization Servers	Operate identity providers and authorization servers to perform authentication and authorization decisions in accordance with [Assignment: organization-defined identity and access management policy].	IA-13	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
IA	IA-13(01)	IA-13(1)	Protection of Cryptographic Keys	Protect the keys used by identity providers that are used for cryptographic operations in accordance with the following controls: [Assignment: organization-defined controls].	IA-13(1)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
IA	IA-13(02)	IA-13(2)	Verification of Identity and Access Tokens	Verify the identity of individuals and access tokens are verified before granting access to [Assignment: organization-defined identity and access tokens].	IA-13(2)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
IA	IA-13(03)	IA-13(3)	Token Management	Manage the following types of identity and access tokens: [Assignment: organization-defined types of identity and access tokens]; and Verify the identity of individuals and access tokens are verified before granting access to [Assignment: organization-defined identity and authentication policy]; assertions and access tokens are generated both issued; c. refreshed; and d. revoked.	IA-13(3)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
IR	IR-01	IR-1	Policy and Procedures	(a) Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one): Organization-level; Mission/business process-level; System-level] incident response policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the incident response policy and the associated incident response controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the incident response policy and procedures; and c. Review and update the current incident response: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	IR-1	Low	Functional	Intersects With	5	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	IR-1	IR-1	IR-1	IR-1	IR-01	IR-01	IR-01	IR-01	IR-1	IR-1	IR-1	IR-1	IR-1	IR-01	IR-01	IR-01		IR-01
IR	IR-01	IR-1	Policy and Procedures	(a) Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one): Organization-level; Mission/business process-level; System-level] incident response policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the incident response policy and the associated incident response controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the incident response policy and procedures; and c. Review and update the current incident response: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	IR-1	Low	Functional	Subset Of	10	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	IR-1	IR-1	IR-1	IR-1	IR-01	IR-01	IR-01	IR-01	IR-1	IR-1	IR-1	IR-1	IR-1	IR-01	IR-01	IR-01		IR-01
IR	IR-01	IR-1	Policy and Procedures	(a) Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one): Organization-level; Mission/business process-level; System-level] incident response policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the incident response policy and the associated incident response controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the incident response policy and procedures; and c. Review and update the current incident response: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	IR-1	Low	Functional	Intersects With	5	IRP Update	IRO-04.2	Mechanisms exist to regularly review and modify incident response practices to incorporate lessons learned, business process changes and industry developments, as necessary.	IR-1	IR-1	IR-1	IR-1	IR-01	IR-01	IR-01	IR-01	IR-1	IR-1	IR-1	IR-1	IR-1	IR-01	IR-01	IR-01		IR-01
IR	IR-01	IR-1	Policy and Procedures	(a) Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one): Organization-level; Mission/business process-level; System-level] incident response policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the incident response policy and the associated incident response controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the incident response policy and procedures; and c. Review and update

Family	Sorting Control #	Focal Document Element	Focal Document Element Name	Focal Document Element Description	NIST SP 800-53 R5.2	Security Control Baseline	Set Theory Relationship Mapping (STRM) Rationale	Set Theory Relationship Mapping (STRM) Relationship	Set Theory Relationship Mapping (STRM) Strength of Relationship	Reference Document Element	Reference Document Name	Reference Document Element Description	NIST SP 800-53 R5.2 Baselines Low	Mod	High	Privacy	FedRAMP R5 Low	Mod	High	LI-SaaS	NIST SP 800-161 R1 C-SCRM Baseline	Low Impact Software Down	Level 1	Level 2	Level 3	GovRAMP Low	Low+	Moderate	Core	High (FedRAMP Rev. 4)
IR	IR-04(13)	IR-4(13)	Incident Handling | Behavior Analysis	Analyze anomalous or suspected adversarial behavior in or related to [Assignment: organization-defined	IR-4(13)	Not Selected	Functional	Intersects With	5	Honeyclients	SEA-12	Mechanisms exist to utilize honeyclients that proactively seek to identify malicious websites and/or web-based malicious code.	IR-4(13)	IR-4(13)	IR-4(13)	IR-4(13)	IR-04(13)	IR-04(13)	IR-04(13)	IR-04(13)	IR-4(13)	IR-4(13)	IR-4(13)	IR-4(13)	IR-4(13)					
IR	IR-04(14)	IR-4(14)	Incident Handling | Security Operations Center	Establish and maintain a security operations center.	IR-4(14)	Not Selected	Functional	Equal	10	Security Operations Center (SOC)	OPS-04	Mechanisms exist to establish and maintain a Security Operations Center (SOC) that facilitates a 24x7 response capability.																		
IR	IR-04(15)	IR-4(15)	Incident Handling | Public Relations and Reputation Repair	Manage public relations associated with an incident; and	IR-4(15)	Not Selected	Functional	Equal	10	Public Relations & Reputation Repair	IRO-16	Mechanisms exist to proactively manage public relations associated with incidents and employ appropriate measures to prevent further reputational damage and develop plans to repair any damage to the organization's reputation.																		
IR	IR-05	IR-5	Incident Monitoring	Track and document incidents.	IR-5	Low	Functional	Equal	10	Situational Awareness For Incidents	IRO-09	Mechanisms exist to document, monitor and report the status of cybersecurity and data protection incidents to internal stakeholders all the way through the resolution of the incident.	IR-5	IR-5	IR-5	IR-5	IR-05	IR-05	IR-05	IR-05	IR-5		IR-5	IR-5	IR-5	IR-05	IR-05	IR-05		IR-05
IR	IR-05(01)	IR-5(1)	Incident Monitoring | Automated Tracking, Data Collection, and Analysis	Track incidents and collect and analyze incident information using [Assignment: organization-defined	IR-5(1)	High	Functional	Equal	10	Automated Tracking, Data Collection & Analysis	IRO-09.1	Automated mechanisms exist to assist in the tracking, collection and analysis of information from actual and potential cybersecurity and data protection incidents.							IR-05(01)											IR-05(01)
IR	IR-06	IR-6	Incident Reporting	Require personnel to report suspected incidents to the organizational incident response capability within [Assignment: organization-defined time period]; andb. Report incident information to [Assignment: organization-defined personnel or roles].	IR-6	Low	Functional	Intersects With	5	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	IR-6	IR-6	IR-6	IR-6	IR-06	IR-06	IR-06	IR-06	IR-6	IR-6	IR-6	IR-6	IR-6	IR-06	IR-06	IR-06	IR-06	IR-06
IR	IR-06	IR-6	Incident Reporting	Report suspected incidents to the organizational incident response capability within [Assignment: organization-defined time period]; andb. Report incident information to [Assignment: organization-defined authorities].	IR-6	Low	Functional	Intersects With	5	Regulatory & Law Enforcement Contacts	IRO-14	Mechanisms exist to maintain incident response contacts with applicable regulatory and law enforcement agencies.	IR-6	IR-6	IR-6	IR-6	IR-06	IR-06	IR-06	IR-06	IR-6	IR-6	IR-6	IR-6	IR-6	IR-06	IR-06	IR-06	IR-06	IR-06
IR	IR-06	IR-6	Incident Reporting	Report suspected incidents to the organizational incident response capability within [Assignment: organization-defined time period]; andb. Report incident information to [Assignment: organization-defined authorities].	IR-6	Low	Functional	Intersects With	5	Contacts With Authorities	GOV-06	Mechanisms exist to identify and document appropriate contacts with relevant law enforcement and regulatory bodies.	IR-6	IR-6	IR-6	IR-6	IR-06	IR-06	IR-06	IR-06	IR-6	IR-6	IR-6	IR-6	IR-6	IR-06	IR-06	IR-06	IR-06	IR-06
IR	IR-06(01)	IR-6(1)	Incident Reporting | Automated Reporting	Report incident information using [Assignment: organization-defined automated mechanisms].	IR-6(1)	Moderate	Functional	Equal	10	Automated Reporting	IRO-10.1	Automated mechanisms exist to assist in the reporting of cybersecurity and data protection incidents.			IR-6(1)	IR-6(1)			IR-06(01)	IR-06(01)				IR-7(2)		IR-7(2)		IR-07(02)	IR-07(02)		IR-06(01)	IR-06(01)
IR	IR-06(02)	IR-6(2)	Incident Reporting | Vulnerabilities Related to Incidents	Report incidents to [Assignment: organization-defined personnel or roles].	IR-6(2)	Not Selected	Functional	Intersects With	5	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	IR-6(2)	IR-6(2)	IR-6(2)	IR-6(2)	IR-06(02)	IR-06(02)	IR-06(02)	IR-06(02)	IR-6(2)	IR-6(2)	IR-6(2)	IR-6(2)	IR-6(2)					
IR	IR-06(02)	IR-6(2)	Incident Reporting | Vulnerabilities Related to Incidents	Report incidents to [Assignment: organization-defined personnel or roles].	IR-6(2)	Not Selected	Functional	Intersects With	5	Vulnerabilities Related To Incidents	IRO-10.3	Mechanisms exist to report system vulnerabilities associated with reported cybersecurity and data protection incidents to organization-defined personnel or roles.	IR-6(2)	IR-6(2)	IR-6(2)	IR-6(2)	IR-06(02)	IR-06(02)	IR-06(02)	IR-06(02)	IR-6(2)	IR-6(2)	IR-6(2)	IR-6(2)	IR-6(2)					
IR	IR-06(03)	IR-6(3)	Incident Reporting | Supply Chain Coordination	Provide incident information to the provider of a product or service and other organizations involved in the supply chain or supply chain governance for systems or system components that experience an incident.	IR-6(3)	Moderate	Functional	Intersects With	5	Supply Chain Coordination	IRO-10.4	Mechanisms exist to provide cybersecurity and data protection incident information to the provider of the Technology Assets, Applications and/or Services (TAAS) and other organizations involved in the supply chain for systems or system components related to the incident.			IR-6(3)	IR-6(3)			IR-06(03)	IR-06(03)			IR-6(3)			IR-6(3)					
IR	IR-07	IR-7	Incident Response Assistance	Provide an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the system for the handling and reporting of incidents.	IR-7	Low	Functional	Equal	10	Incident Reporting Assistance	IRO-11	Mechanisms exist to provide incident response advice and assistance to users of Technology Assets, Applications and/or Services (TAAS) for the handling and reporting of actual and potential cybersecurity and data protection incidents.	IR-7	IR-7	IR-7	IR-7	IR-07	IR-07	IR-07	IR-07						IR-07	IR-07	IR-07		IR-07
IR	IR-07(01)	IR-7(1)	Incident Response Assistance | Automation Support for Availability of Information and Support	Increase the availability of incident response information and support using [Assignment: organization-defined automated mechanisms].	IR-7(1)	Moderate	Functional	Equal	10	Automation Support of Availability of Information / Support	IRO-11.1	Automated mechanisms exist to increase the availability of incident response-related information and support.			IR-7(1)	IR-7(1)			IR-07(01)	IR-07(01)								IR-07(01)			IR-07(01)
IR	IR-07(02)	IR-7(2)	Incident Response Assistance | Coordination with External Providers	Establish a direct, cooperative relationship between the organization's incident response capability and external service providers;	IR-7(2)	Not Selected	Functional	Equal	10	Coordination With External Providers	IRO-11.2	Mechanisms exist to establish a direct, cooperative relationship between the organization's incident response capability and external service providers.									IR-7(2)			IR-7(2)		IR-07(02)	IR-07(02)		IR-07(02)
IR	IR-08	IR-8	Incident Response Plan	Develop an incident response plan that: a. Provides the organization with a roadmap for implementing its incident response capability; b. Describes the structure and organization of the incident response capability; c. Provides a high-level approach for how the incident response capability fits into the overall organization; d. Defines reportable incidents; e. Addresses the sharing of incident information; f. Defines the resources and management support needed to effectively maintain and mature an incident response capability; g. Addresses the need for data privacy protections throughout the incident response process; h. Is reviewed and approved by [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency]; and i. Explicitly designates responsibility for incident response to [Assignment: organization-defined personnel or roles].	IR-8	Low	Functional	Equal	10	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	IR-8	IR-8	IR-8	IR-8	IR-08	IR-08	IR-08	IR-08	IR-8	IR-8		IR-8	IR-8	IR-08	IR-08	IR-08	IR-08	IR-08
IR	IR-08(01)	IR-8(1)	Incident Response Plan | Breaches	Include the following in the Incident Response Plan for breaches involving personally identifiable information: a. A process to determine if notice is needed;b. An assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms; andc. Identification of applicable privacy requirements.	IR-8(1)	Not Selected	Functional	Equal	10	Data Breach	IRO-04.1	Mechanisms exist to address data breaches, or other incidents involving the unauthorized disclosure of sensitive or regulated data, according to applicable laws, regulations and contractual obligations.				IR-8(1)															
IR	IR-09	IR-9	Information Spillage Response	Respond to information spills by: a. Assigning [Assignment: organization-defined personnel or roles] with the responsibility to respond to information spills; b. Identifying the specific information involved in the system contamination; c. Alerting [Assignment: organization-defined personnel or roles] of the information spill using a method of communication not associated with the spill;d. Isolating the contaminated system or system component; e. Eradicating the information from the contaminated system or component; f. Identifying other systems or system components that may have been subsequently contaminated; and g. Performing the following additional actions after the information spill: [Assignment: organization-defined actions].	IR-9	Not Selected	Functional	Intersects With	5	Information Spillage Response	IRO-12	Mechanisms exist to respond to sensitive information spills.	IR-9	IR-9	IR-9	IR-9	IR-09	IR-09	IR-09	IR-09	IR-9	IR-9	IR-9	IR-9	IR-9		IR-09	IR-09		IR-09
IR	IR-09	IR-9	Information Spillage Response	Respond to information spills by: a. Assigning [Assignment: organization-defined personnel or roles] with the responsibility to respond to information spills; b. Identifying the specific information involved in the system contamination; c. Alerting [Assignment: organization-defined personnel or roles] of the information spill using a method of communication not associated with the spill;d. Isolating the contaminated system or system component; e. Eradicating the information from the contaminated system or component; f. Identifying other systems or system components that may have been subsequently contaminated; and g. Performing the following additional actions after the information spill: [Assignment: organization-defined actions].	IR-9	Not Selected	Functional	Intersects With	5	Responsible Personnel	IRO-12.1	Mechanisms exist to formally assign personnel or roles with responsibility for responding to sensitive information spills.	IR-9	IR-9	IR-9	IR-9	IR-09	IR-09	IR-09	IR-09	IR-9	IR-9	IR-9	IR-9	IR-9		IR-09	IR-09		IR-09
IR	IR-09(01)	IR-9(1)	Withdrawn	Withdrawn	IR-9(1)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A														IR-09(01)	IR-09(01)			IR-09(01)
IR	IR-09(02)	IR-9(2)	Information Spillage Response | Training	Provide information spillage response training [Assignment: organization-defined frequency].	IR-9(2)	Not Selected	Functional	Equal	10	Training	IRO-12.2	Mechanisms exist to ensure incident response training material provides coverage for sensitive information spillage response.						IR-09(02)	IR-09(02)									IR-09(02)			IR-09(02)
IR	IR-09(03)	IR-9(3)	Information Spillage Response | Post-spill Operations	Implement the following procedures to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions: [Assignment: organization-defined procedures].	IR-9(3)	Not Selected	Functional	Equal	10	Post-Sensitive / Regulated Data Spill Operations	IRO-12.3	Mechanisms exist to ensure that organizational personnel impacted by sensitive/regulated data spills can continue to carry out assigned tasks while contaminated Technology Assets, Applications and/or Services (TAAS) are undergoing corrective actions.						IR-09(03)	IR-09(03)									IR-09(03)			IR-09(03)
IR	IR-09(04)	IR-9(4)	Information Spillage Response | Exposure to Unauthorized Personnel	Employ the following controls for personnel exposed to information not within assigned access authorizations: [Assignment: organization-defined controls].	IR-9(4)	Not Selected	Functional	Equal	10	Exposure to Unauthorized Personnel	IRO-12.4	Mechanisms exist to address security safeguards for personnel exposed to sensitive information that is not within their assigned access authorizations.						IR-09(04)	IR-09(04)									IR-09(04)			IR-09(04)
IR	IR-10	IR-10	Withdrawn	Withdrawn	IR-10	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
MA	MA-01	MA-1	Policy and Procedures	Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: a. [Selection (one or more): Organization-level; Mission/business process-level; System-level] maintenance policy that: 1. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and b. Procedures to facilitate the implementation of the maintenance policy and the associated maintenance controls; c. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the maintenance policy and procedures; and d. Review and update the current maintenance: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	MA-1	Low	Functional	Subset Of	10	Maintenance Operations	MNT-01	Mechanisms exist to develop, disseminate, review & update procedures to facilitate the implementation of maintenance controls across the enterprise.	MA-1	MA-1	MA-1	MA-1	MA-01	MA-01	MA-01	MA-01	MA-1	MA-1	MA-1	MA-1	MA-1	MA-01	MA-01	MA-01		MA-01
MA	MA-01	MA-1	Policy and Procedures	Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: a. [Selection (one or more): Organization-level; Mission/business process-level; System-level] maintenance policy that: 1. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and b. Procedures to facilitate the implementation of the maintenance policy and the associated maintenance controls; c. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the maintenance policy and procedures; and d. Review and update the current maintenance: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	MA-1	Low	Functional	Intersects With	5	Remote Maintenance Notifications	MNT-05.2	Mechanisms exist to require maintenance personnel to notify affected stakeholders when remote, non-local maintenance is planned (e.g., date/time).	MA-1	MA-1	MA-1	MA-1	MA-01	MA-01	MA-01	MA-01	MA-1	MA-1	MA-1	MA-1	MA-1	MA-01	MA-01	MA-01		MA-01
MA	MA-01	MA-1	Policy and Procedures	Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: a. [Selection (one or more): Organization-level; Mission/business process-level; System-level] maintenance policy that: 1. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and b. Procedures to facilitate the implementation of the maintenance policy and the associated maintenance controls; c. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the maintenance policy and procedures; and d. Review and update the current maintenance: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	MA-1	Low	Functional	Intersects With	5	Auditing Remote Maintenance	MNT-05.1	Mechanisms exist to audit remote, non-local maintenance and diagnostic sessions, as well as review the maintenance action performed during remote maintenance sessions.	MA-1	MA-1	MA-1	MA-1	MA-01	MA-01	MA-01	MA-01	MA-1	MA-1	MA-1	MA-1	MA-1	MA-01	MA-01	MA-01		MA-01
MA	MA-01	MA-1	Policy and Procedures	Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: a. [Selection (one or more): Organization-level; Mission/business process-level; System-level] maintenance policy that: 1. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and b. Procedures to facilitate the implementation of the maintenance policy and the associated maintenance controls; c. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the maintenance policy and procedures; and d. Review and update the current maintenance: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	MA-1	Low	Functional	Intersects With	5	Cybersecurity & Data Protection Governance Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	MA-1	MA-1	MA-1	MA-1	MA-01	MA-01	MA-01	MA-01	MA-1	MA-1	MA-1	MA-1	MA-1	MA-01	MA-01	MA-01		MA-01
MA	MA-01	MA-1	Policy and Procedures	Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: a. [Selection (one or more): Organization-level; Mission/business process-level; System-level] maintenance policy that: 1. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and b. Procedures to facilitate the implementation of the maintenance policy and the associated maintenance controls; c. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the maintenance policy and procedures; and d. Review and update the current maintenance: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	MA-1	Low	Functional	Intersects With	5	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	MA-1	MA-1	MA-1	MA-1	MA-01	MA-01	MA-01	MA-01	MA-1	MA-1	MA-1	MA-1	MA-1	MA-01	MA-01	MA-01		MA-01
MA	MA-02	MA-2	Controlled Maintenance	Schedule, perform, document, and review records of maintenance, repair, and replacement on system components in accordance with manufacturer or vendor specifications and/or organizational requirements; b. Approve and monitor all maintenance activities, whether performed on site or remotely and whether the system or system components are serviced on site or removed to another location; c. Require that [Assignment: organization-defined personnel or roles] explicitly approve the removal of the system or system components from organizational facilities for off-site maintenance, repair, or replacement; d. Sanitize equipment to remove the following information from associated media prior to removal from organizational facilities for off-site maintenance, repair, or replacement: [Assignment: organization-defined information]; e. Check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions; and f. Include the following information in organizational maintenance records: [Assignment: organization-defined information].	MA-2	Low	Functional	Equal	10	Controlled Maintenance	MNT-02	Mechanisms exist to conduct controlled maintenance activities throughout the lifecycle of the Technology Asset, Application and/or Service (TAAS).	MA-2	MA-2	MA-2		MA-02	MA-02	MA-02	MA-02						MA-02	MA-02	MA-02		MA-02
MA	MA-02(01)	MA-2(1)	Withdrawn	Withdrawn	MA-2(1)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
MA	MA-02(02)	MA-2(2)	Controlled Maintenance | Automated Maintenance Activities	Schedule, conduct, and document maintenance, repair, and replacement actions for the system using [Assignment: organization-defined automated mechanisms]; andb. Produce up-to date, accurate, and complete records of all maintenance, repair, and replacement actions requested, scheduled, in process, and completed.	MA-2(2)	High	Functional	Equal	10	Automated Maintenance Activities	MNT-02.1	Automated mechanisms exist to schedule, conduct and document maintenance and repairs.			MA-2(2)				MA-02(02)						MA-2(2)					MA-02(02)
MA	MA-03	MA-3	Maintenance Tools	Approve, control, and monitor the use of system maintenance tools.	MA-3	Moderate	Functional	Intersects With	5	Maintenance Tools	MNT-04	Mechanisms exist to control and monitor the use of system maintenance tools.		MA-3	MA-3			MA-03	MA-03					MA-3	MA-3			MA-03	MA-03	MA-03	MA-03
MA	MA-03(01)	MA-3(1)	Maintenance Tools | Inspect Tools	Inspect the maintenance tools used by maintenance personnel for improper or unauthorized modifications.	MA-3(1)	Moderate	Functional	Equal	10	Inspect Tools	MNT-04.1	Mechanisms exist to inspect maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.		MA-3(1)	MA-3(1)			MA-03(01)	MA-03(01)					MA-3(1)			MA-03(01)	MA-03(01)		MA-03(01)
MA	MA-03(02)	MA-3(2)	Maintenance Tools | Inspect Media	Check media containing diagnostic and test programs for malicious code before the media are used in the system.	MA-3(2)	Moderate	Functional	Equal	10	Inspect Media	MNT-04.2	Mechanisms exist to check media containing diagnostic and test programs for malicious code before the media are used.		MA-3(2)	MA-3(2)			MA-03(02)	MA-03(02)					MA-3(2)				MA-03(02)		MA-03(02)
MA	MA-03(03)	MA-3(3)	Maintenance Tools | Prevent Unauthorized Removal	Prevent the unauthorized removal of maintenance equipment and/or software by: a. Verifying that there is no organizational information contained on the equipment;b. Sanitizing or destroying the equipment;c. Retaining the equipment within the facility; or d. Obtaining an exemption from [Assignment: organization-defined personnel or roles] explicitly authorizing removal of the equipment from the facility.	MA-3(3)	Moderate	Functional	Equal	10	Prevent Unauthorized Removal	MNT-04.3	Mechanisms exist to prevent or control the removal of equipment undergoing maintenance that contains organizational information.		MA-3(3)	MA-3(3)			MA-03(03)	MA-03(03)					MA-3(3)				MA-03(03)		MA-03(03)
MA	MA-03(04)	MA-3(4)	Maintenance Tools | Restricted Tool Use	Restrict the use of maintenance tools to authorized personnel only.	MA-3(4)	Not Selected	Functional	Equal	10	Restrict Tool Usage	MNT-04.4	Automated mechanisms exist to restrict the use of maintenance tools to authorized maintenance personnel and/or roles.																		
MA	MA-03(05)	MA-3(5)	Maintenance Tools | Execution with Privilege	Monitor the use of maintenance tools that execute with increased privilege.	MA-3(5)	Not Selected	Functional	Intersects With	5	Maintenance Tools	MNT-04	Mechanisms exist to control and monitor the use of system maintenance tools.																		
MA	MA-03(06)	MA-3(6)	Maintenance Tools | Software Updates and Patches	Inspect maintenance tools to ensure the latest software updates and patches are installed.	MA-3(6)	Not Selected	Functional	Intersects With	5	Maintenance Tools	MNT-04	Mechanisms exist to control and monitor the use of system maintenance tools.																		
MA	MA-04	MA-4	Nonlocal Maintenance	Approve and monitor nonlocal maintenance and diagnostic sessions; b. Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions; c. Maintain records for nonlocal maintenance and diagnostic activities; and d. Terminate session and network connections when nonlocal maintenance is completed.	MA-4	Low	Functional	Intersects With	5	Remote Maintenance	MNT-05	Mechanisms exist to authorize, monitor and control remote, non-local maintenance and diagnostic activities.	MA-4	MA-4	MA-4	MA-4	MA-04	MA-04	MA-04	MA-04	MA-4	MA-4	MA-4	MA-4	MA-4	MA-04	MA-04	MA-04		MA-04
MA	MA-04	MA-4	Nonlocal Maintenance	Approve and monitor nonlocal maintenance and diagnostic sessions; b. Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions; c. Maintain records for nonlocal maintenance and diagnostic activities; and d. Terminate session and network connections when nonlocal maintenance is completed.	MA-4	Low	Functional	Intersects With	5	Remote Maintenance Notifications	MNT-05.2	Mechanisms exist to require maintenance personnel to notify affected stakeholders when remote, non-local maintenance is planned (e.g., date/time).	MA-4	MA-4	MA-4	MA-4	MA-04	MA-04	MA-04	MA-04	MA-4	MA-4	MA-4	MA-4	MA-4	MA-04	MA-04	MA-04		MA-04
MA	MA-04	MA-4	Nonlocal Maintenance	Approve and monitor nonlocal maintenance and diagnostic sessions; b. Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions; c. Maintain records for nonlocal maintenance and diagnostic activities; and d. Terminate session and network connections when nonlocal maintenance is completed.	MA-4	Low	Functional	Intersects With	5	Auditing Remote Maintenance	MNT-05.1	Mechanisms exist to audit remote, non-local maintenance and diagnostic sessions, as well as review the maintenance action performed during remote maintenance sessions.	MA-4	MA-4	MA-4	MA-4	MA-04	MA-04	MA-04	MA-04	MA-4	MA-4	MA-4	MA-4	MA-4	MA-04	MA-04	MA-04		MA-04
MA	MA-04(01)	MA-4(1)	Nonlocal Maintenance | Logging and Review	Log the date and time of nonlocal maintenance and diagnostic sessions; and b. Review the audit records of the maintenance and diagnostic sessions.	MA-4(1)	Not Selected	Functional	Intersects With	5	Auditing Remote Maintenance	MNT-05.1	Mechanisms exist to audit remote, non-local maintenance and diagnostic sessions, as well as review the maintenance action performed during remote maintenance sessions.																		
MA	MA-04(02)	MA-4(2)	Withdrawn	Withdrawn	MA-4(2)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																MA-04(02)		MA-04(02)
MA	MA-04(03)	MA-4(3)	Nonlocal Maintenance | Comparable Security and Sanitization	Require that the component to be serviced is purged of all data, firmware, and software before the component is removed from organizational facilities; and b. After the service is complete, sanitize the component and restore the component to the previously configured state before reconnecting the component to the system.	MA-4(3)	High	Functional	Equal	10	Remote Maintenance Comparable Security & Sanitization	MNT-05.6	Mechanisms exist to require Technology Assets, Applications and/or Services (TAAS) performing remote, non-local maintenance and/or diagnostic services implement a security capability comparable to the capability implemented on the TAAS being serviced.			MA-4(3)				MA-04(03)				MA-4(3)	MA-4(3)						MA-04(03)
MA	MA-04(04)	MA-4(4)	Nonlocal Maintenance | Authentication and Separation of Maintenance Sessions	Protect nonlocal maintenance sessions by: a. Employing [Assignment: organization-defined authenticators that are replay resistant]; and b. Separating the maintenance sessions from other network sessions with the system by logically separated communications paths or physically separated communications paths.	MA-4(4)	Not Selected	Functional	Equal	10	Separation of Maintenance Sessions	MNT-05.7	Mechanisms exist to protect maintenance sessions through replay-resistant sessions that are physically or logically separated communications paths from other network sessions.																		
MA	MA-04(05)	MA-4(5)	Nonlocal Maintenance | Approvals and Notifications	Require the approval of each nonlocal maintenance session by [Assignment: organization-defined personnel or roles]; andb. Notify the following personnel or roles of nonlocal maintenance sessions: [Assignment: organization-defined personnel or roles].	MA-4(5)	Not Selected	Functional	Equal	10	Remote Maintenance Pre-Approval	MNT-05.5	Mechanisms exist to require maintenance personnel to obtain pre-approval and scheduling for remote, non-local maintenance sessions.																		
MA	MA-04(06)	MA-4(6)	Nonlocal Maintenance | Cryptographic Protection	Implement the following cryptographic mechanisms to protect the integrity and confidentiality of nonlocal maintenance and diagnostic communications: [Assignment: organization-defined cryptographic mechanisms].	MA-4(6)	Not Selected	Functional	Equal	10	Remote Maintenance Cryptographic Protection	MNT-05.3	Cryptographic mechanisms exist to protect the integrity and confidentiality of remote, non-local maintenance and diagnostic communications.																		MA-04(06)
MA	MA-04(07)	MA-4(7)	Nonlocal Maintenance | Disconnect Verification	Verify session and network connection termination after the completion of nonlocal maintenance and diagnostic sessions.	MA-4(7)	Not Selected	Functional	Equal	10	Remote Maintenance Disconnect Verification	MNT-05.4	Mechanisms exist to provide remote disconnect verification to ensure remote, non-local maintenance and diagnostic sessions are properly terminated.																		
MA	MA-05	MA-5	Maintenance Personnel	Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance personnel. The process must ensure that all maintenance personnel possess the required access authorizations;	MA-5	Low	Functional	Equal	10	Authorized Maintenance Personnel	MNT-06	Mechanisms exist to maintain a current list of authorized maintenance organizations or personnel.	MA-5	MA-5	MA-5		MA-05	MA-05	MA-05	MA-05	MA-5		MA-5	MA-5	MA-5	MA-05	MA-05	MA-05		MA-05
MA	MA-05(01)	MA-5(1)	Maintenance Personnel | Individuals Without Appropriate Access	Maintenance personnel without appropriate access authorizations, and who are technically qualified; and2. Prior to initiating maintenance or diagnostic activities by personnel without appropriate access authorizations, all volatile information storage components within the system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured.	MA-5(1)	High	Functional	Intersects With	5	Maintenance Personnel Without Appropriate Access	MNT-06.1	Mechanisms exist to ensure the risks associated with maintenance personnel who do not have appropriate access authorizations, clearances or formal access approvals are appropriately mitigated.				MA-5(1)				MA-05(01)	MA-05(01)								MA-05(01)		MA-05(01)
MA	MA-05(02)	MA-5(2)	Maintenance Personnel | Security Clearances for Classified Systems	Verify that personnel have valid access authorizations and security clearances before performing maintenance on classified systems; and b. Verify that personnel have the required access authorizations before granting access to the system.	MA-5(2)	Not Selected	Functional	Intersects With	5	Maintenance Personnel Without Appropriate Access	MNT-06.1	Mechanisms exist to ensure the risks associated with maintenance personnel who do not have appropriate access authorizations, clearances or formal access approvals are appropriately mitigated.																		
MA	MA-05(03)	MA-5(3)	Maintenance Personnel | Citizenship Requirements for Classified Systems	Verify that personnel have valid access authorizations and security clearances before performing maintenance and diagnostic activities on a system processing, storing, or transmitting classified information; and b. Verify that personnel have the required access authorizations before granting access to the system.	MA-5(3)	Not Selected	Functional	Intersects With	5	Maintenance Personnel Without Appropriate Access	MNT-06.1	Mechanisms exist to ensure the risks associated with maintenance personnel who do not have appropriate access authorizations, clearances or formal access approvals are appropriately mitigated.																		
MA	MA-05(04)	MA-5(4)	Maintenance Personnel | Foreign Nationals	Verify that: a. For classified systems, only U.S. citizens are authorized for maintenance and diagnostic activities; and b. For nonclassified systems, personnel performing maintenance and diagnostic activities meet organizational personnel screening requirements.	MA-5(4)	Not Selected	Functional	Intersects With	5	Maintenance Personnel Without Appropriate Access	MNT-06.1	Mechanisms exist to ensure the risks associated with maintenance personnel who do not have appropriate access authorizations, clearances or formal access approvals are appropriately mitigated.								MA-5(4)		MA-5(4)	MA-5(4)							
MA	MA-05(05)	MA-5(5)	Maintenance Personnel | Non-system Maintenance	Ensure that non-escorted personnel performing maintenance activities not directly associated with the system but in the physical proximity of the system, have required access authorizations.	MA-5(5)	Not Selected	Functional	Equal	10	Non-System Related Maintenance	MNT-06.2	Mechanisms exist to ensure that non-escorted personnel performing non-IT maintenance activities in the physical proximity of systems have required access authorizations.																		
MA	MA-06	MA-6	Timely Maintenance	Obtain maintenance support and/or spare parts for [Assignment: organization-defined system components] within [Assignment: organization-defined time period] of failure.	MA-6	Moderate	Functional	Equal	10	Timely Maintenance	MNT-03	Mechanisms exist to obtain maintenance support and/or spare parts for Technology Assets, Applications and/or Services (TAAS) within a defined Recovery Time Objective (RTO).			MA-

Family	Sorting Control #	Focal Document Element	Focal Document Element Name	Focal Document Element Description	NIST SP 800-53 R5.2	Security Control Baseline	Set Theory Relationship Mapping (STRM) Rationale	Relationship	Strength of Relationship	Reference Document Element	Reference Document Name	Reference Document Element Description	NIST SP 800-53 R5.2 Baselines Low	Mod	High	Privacy	FedRAMP R5 Low	Mod	High	LI-SaaS	NIST SP 800-161 R1 C-SCRM Baseline	Key Supply Chain Controls	Level 1	Level 2	Level 3	GovRAMP Low	Low+	Moderate	Core	High (FedRAMP Only)
MP	MP-08(01)	MP-8(1)	Media Downgrading | Documentation of Process	Document system media downgrading actions.	MP-8(1)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
MP	MP-08(02)	MP-8(2)	Media Downgrading | Equipment Testing	Test downgrading equipment and procedures [Assignment: organization-defined frequency] to ensure downgrade system media containing controlled unclassified information prior to public release.	MP-8(2)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
MP	MP-08(03)	MP-8(3)	Media Downgrading | Controlled Unclassified Information	Apply downgrading procedures to remove information prior to release to individuals without [Assignment: organization-defined controlled unclassified information access agreements].	MP-8(3)	Not Selected	Functional	Intersects With	5	Data Reclassification	DCH-11	Mechanisms exist to reclassify data, including associated Technology Assets, Applications and/or Services (TAAS), commensurate with the security category and/or classification level of the information.																		
MP	MP-08(04)	MP-8(4)	Media Downgrading | Classified Information	Document system media downgrading actions.	MP-8(4)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
PE	PE-01	PE-1	Policy and Procedures	Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: [Assignment: organization-defined physical and environmental protection policy and the associated physical and environmental protection controls]; and [Assignment: organization-defined personnel or roles] with the [Assignment: organization-defined frequency]:	PE-1	Low	Functional	Intersects With	5	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	PE-1	PE-1	PE-1	PE-1	PE-01	PE-01	PE-01	PE-01	PE-1	PE-1	PE-1	PE-1	PE-1	PE-01	PE-01	PE-01		PE-01
PE	PE-01	PE-1	Policy and Procedures	Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: [Assignment: organization-defined physical and environmental protection policy and the associated physical and environmental protection controls]; and [Assignment: organization-defined personnel or roles] with the [Assignment: organization-defined frequency]:	PE-1	Low	Functional	Subset Of	10	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	PE-1	PE-1	PE-1	PE-1	PE-01	PE-01	PE-01	PE-01	PE-1	PE-1	PE-1	PE-1	PE-1	PE-01	PE-01	PE-01		PE-01
PE	PE-01	PE-1	Policy and Procedures	Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: [Assignment: organization-defined physical and environmental protection policy and the associated physical and environmental protection controls]; and [Assignment: organization-defined personnel or roles] with the [Assignment: organization-defined frequency]:	PE-1	Low	Functional	Intersects With	5	Cybersecurity & Data Protection Governance Program	GOV-03	Mechanisms exist to develop, report on and monitor a cybersecurity and data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	PE-1	PE-1	PE-1	PE-1	PE-01	PE-01	PE-01	PE-01	PE-1	PE-1	PE-1	PE-1	PE-1	PE-01	PE-01	PE-01		PE-01
PE	PE-02	PE-2	Physical Access Authorizations	Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides (except for those areas within the facility officially designated as publicly accessc. Review the access list detailing authorized	PE-2	Low	Functional	Equal	10	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly	PE-2	PE-2	PE-2		PE-02	PE-02	PE-02	PE-02	PE-2	PE-2		PE-2	PE-2	PE-02	PE-02	PE-02		PE-02
PE	PE-02(01)	PE-2(1)	Physical Access Authorizations | Access by Position or Role	Authorize physical access to the facility where the system resides based on position or role.	PE-2(1)	Not Selected	Functional	Equal	10	Role-Based Physical Access	PES-02.1	Physical access control mechanisms exist to authorize physical access to facilities based on the position or role of the individual.												PE-2(1)	PE-2(1)					
PE	PE-02(02)	PE-2(2)	Physical Access Authorizations | Two Forms of Identification	Require two forms of identification from the following forms of identification for visitor access to the facility where the system resides: [Assignment: organization-defined list of acceptable forms of identification].	PE-2(2)	Not Selected	Functional	Equal	10	Identification Requirement	PES-06.2	Physical access control mechanisms exist to require at least one (1) form of government-issued or organization-issued photo identification to authenticate individuals before they can gain access to the facility.																		
PE	PE-02(03)	PE-2(3)	Physical Access Authorizations | Restrict Unescorted Access	Restrict unescorted access to the facility where the system resides to personnel with [Selection (one or more): security clearances for all information contained within the system; formal access authorizations for all information contained within the system; need for	PE-2(3)	Not Selected	Functional	Equal	10	Restrict Unescorted Access	PES-06.3	Physical access control mechanisms exist to restrict unescorted access to facilities to personnel with required security clearances, formal access authorizations and validated the need for access.												PE-3(5)	PE-3(5)					
PE	PE-03	PE-3	Physical Access Control	Enforce physical access authorizations at [Assignment: organization-defined entry and exit points to the facility where the system resides] by: Verifying individual access authorizations before granting access to the facility; and Controlling ingress and egress to the facility using [Selection (one or more): [Assignment: organization-defined physical access control systems or devices]; guards];	PE-3	Low	Functional	Intersects With	5	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access to facilities (excluding those areas within the facility officially designated as publicly accessible) by validating physical access authorizations for all personnel, including visitors, before granting access to facility (excluding those areas within the facility officially designated as publicly accessible).	PE-3	PE-3	PE-3		PE-03	PE-03	PE-03	PE-03	PE-3			PE-3	PE-3	PE-03	PE-03	PE-03		PE-03
PE	PE-03(01)	PE-3(1)	Physical Access Control | System Access	Enforce physical access authorizations to the system in addition to the physical access controls for the facility at [Assignment: organization-defined physical spaces containing one or more components of the system].	PE-3(1)	High	Functional	Equal	10	Access To Critical Systems	PES-03.4	Physical access control mechanisms exist to enforce physical access to critical systems or sensitive/regulated data, in addition to the physical access controls for the facility.			PE-3(1)			PE-03(01)						PE-3(1)	PE-3(1)					PE-03(01)
PE	PE-03(02)	PE-3(2)	Physical Access Control | Facility and Systems	Perform security checks [Assignment: organization-defined frequency] at the physical perimeter of the facility or system for exfiltration of information or removal of system components.	PE-3(2)	Not Selected	Functional	Intersects With	5	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access to facilities (excluding those areas within the facility officially designated as publicly accessible) by validating physical access authorizations for all personnel, including visitors, before granting access to facility (excluding those areas within the facility officially designated as publicly accessible).												PE-3(2)	PE-3(2)					
PE	PE-03(03)	PE-3(3)	Physical Access Control | Continuous Guards	Employ [Assignment: organization-defined physical access points] to the facility where the system resides [Assignment: organization-defined frequency] physical security personnel to [Assignment: organization-defined actions or events].	PE-3(3)	Not Selected	Functional	Intersects With	5	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access to facilities (excluding those areas within the facility officially designated as publicly accessible).																		
PE	PE-03(04)	PE-3(4)	Physical Access Control | Lockable Casings	Use lockable physical casings to protect [Assignment: organization-defined system components] from unauthorized physical access.	PE-3(4)	Not Selected	Functional	Equal	10	Lockable Physical Casings	PES-03.2	Physical access control mechanisms exist to protect system components from unauthorized physical access (e.g., lockable physical casings).																		
PE	PE-03(05)	PE-3(5)	Physical Access Control | Logical Tampering Protection	Employ [Assignment: organization-defined security safeguards] to prevent] physical tampering or alteration of [Assignment: organization-defined hardware components within the system].	PE-3(5)	Not Selected	Functional	Equal	10	Mobile Device Tampering	MDM-04	Mobile device management controls exist to protect the confidentiality, integrity and availability of data on mobile devices that are stored on personal or corporate-owned devices, including BYOD devices, that are used to access organizational data and/or systems. Mobile device management controls must be implemented to enforce applicable mobile device restrictions, including: (1) Full-device or container encryption; (2) Configuration management; (3) Application management; (4) Jailbreaking and rooting restrictions; (5) Multi-factor authentication; (6) Remote purging; (7) Malware defense; and (8) Mobile device connection scanning by devices prior to connecting to organizational networks.												PE-3(5)	PE-3(5)					
PE	PE-03(06)	PE-3(6)		Withdrawn	PE-3(6)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
PE	PE-03(07)	PE-3(7)	Physical Access Control | Physical Barriers	Limit access using physical barriers.	PE-3(7)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
PE	PE-03(08)	PE-3(8)	Physical Access Control | Access Control Vestibules	Employ access control vestibules at [Assignment: organization-defined locations within the facility].	PE-3(8)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
PE	PE-04	PE-4	Access Control for Transmission	Control physical access to [Assignment: organization-defined system distribution and transmission lines] within organizational facilities using [Assignment: organization-defined security controls].	PE-4	Moderate	Functional	Equal	10	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.		PE-4	PE-4			PE-04	PE-04							PE-04	PE-04		PE-04
PE	PE-05	PE-5	Access Control for Output Devices	Control physical access to output from [Assignment: organization-defined output devices] to prevent	PE-5	Moderate	Functional	Equal	10	Access Control for Output Devices	PES-12.2	Physical security mechanisms exist to restrict access to printers and other system output devices to prevent unauthorized individuals from obtaining the output.		PE-5	PE-5			PE-05	PE-05							PE-05	PE-05		PE-05
PE	PE-05(01)	PE-5(1)		Withdrawn	PE-5(1)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
PE	PE-05(02)	PE-5(2)	Access Control for Output Devices | Link to Individual Identity	Link individual identity to receipt of output from output devices.	PE-5(2)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
PE	PE-05(03)	PE-5(3)		Withdrawn	PE-5(3)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
PE	PE-06	PE-6	Monitoring Physical Access	Monitor physical access to the facility where the system resides to detect and respond to physical security incidents. Review physical access logs [Assignment: organization-defined frequency] and upon occurrence of [Assignment: organization-defined events or potential indications of events]; and Coordinate results of reviews and investigations with the organization's incident response capability.	PE-6	Low	Functional	Equal	10	Monitoring Physical Access	PES-05	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.	PE-6	PE-6	PE-6		PE-06	PE-06	PE-06	PE-06	PE-6		PE-6	PE-6	PE-6	PE-06	PE-06	PE-06		PE-06
PE	PE-06(01)	PE-6(1)	Monitoring Physical Access | Intrusion Alarms and Surveillance Equipment	Monitor physical intrusion alarms and surveillance equipment.	PE-6(1)	Moderate	Functional	Equal	10	Intrusion Alarms / Surveillance Equipment	PES-05.1	Physical access control mechanisms exist to monitor physical intrusion alarms and surveillance equipment.		PE-6(1)	PE-6(1)			PE-06(01)	PE-06(01)							PE-06(01)			PE-06(01)
PE	PE-06(02)	PE-6(2)	Monitoring Physical Access | Automated Intrusion Recognition and Responses	Recognize [Assignment: organization-defined classes or types of intrusions] and initiate [Assignment: organization-defined response actions] using [Assignment: organization-defined automated mechanisms].	PE-6(2)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
PE	PE-06(03)	PE-6(3)	Monitoring Physical Access | Video Surveillance	Employ video surveillance of [Assignment: organization-defined operational areas] and retain video recordings [Assignment: organization-defined	PE-6(3)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
PE	PE-06(04)	PE-6(4)	Monitoring Physical Access | Monitoring Physical Access to Systems	Monitor physical access to the facility at [Assignment: organization-defined physical spaces containing one or more components of the system].	PE-6(4)	High	Functional	Equal	10	Monitoring Physical Access To Critical Systems	PES-05.2	Facility security mechanisms exist to monitor physical access to critical systems or sensitive/regulated data, in addition to the physical access monitoring of the facility.			PE-6(4)				PE-06(04)											PE-06(04)
PE	PE-07	PE-7		Withdrawn	PE-7	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
PE	PE-08	PE-8	Visitor Access Records	a. Maintain visitor access records to the facility where the system resides for [Assignment: organization-defined time period]; b. Review visitor access records [Assignment: organization-defined frequency]; and c. Report anomalies in visitor access records to [Assignment: organization-defined personnel].	PE-8	Low	Functional	Equal	10	Physical Access Logs	PES-03.3	Physical access control mechanisms generate a log entry for each access attempt through controlled ingress and egress points.	PE-8	PE-8	PE-8		PE-08	PE-08	PE-08	PE-08						PE-08	PE-08	PE-08		PE-08
PE	PE-08(01)	PE-8(1)	Visitor Access Records | Automated Records Maintenance and Review	Maintain and review visitor access records using [Assignment: organization-defined automated mechanisms].	PE-8(1)	High	Functional	Equal	10	Automated Records Management & Review	PES-06.4	Automated mechanisms exist to facilitate the maintenance and review of visitor access records.			PE-8(1)				PE-08(01)											PE-08(01)
PE	PE-08(02)	PE-8(2)		Withdrawn	PE-8(2)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
PE	PE-08(03)	PE-8(3)	Visitor Access Records | Limit Personally Identifiable Information Elements	Limit personally identifiable information contained in visitor access records to the following elements identified in the privacy risk assessment: [Assignment: organization-defined elements].	PE-8(3)	Not Selected	Functional	Equal	10	Minimize Visitor Personal Data (PD)	PES-06.5	Mechanisms exist to minimize the collection of Personal Data (PD) contained in visitor access records.				PE-8(3)														
PE	PE-09	PE-9	Power Equipment and Cabling	Protect power equipment and power cabling for the system from damage and destruction.	PE-9	Moderate	Functional	Equal	10	Supporting Utilities	PES-07	Facility security mechanisms exist to protect power equipment and power cabling for the system from damage and destruction.		PE-9	PE-9			PE-09	PE-09							PE-09			PE-09
PE	PE-09(01)	PE-9(1)	Power Equipment and Cabling | Redundant Cabling	Employ redundant power cabling paths that are physically separated by [Assignment: organization-defined distance].	PE-9(1)	Not Selected	Functional	Equal	10	Redundant Cabling	PES-07.7	Mechanisms exist to employ redundant power cabling paths that are physically separated to ensure that power continues to flow in the event one of the cables is cut or otherwise damaged.																		
PE	PE-09(02)	PE-9(2)	Power Equipment and Cabling | Automatic Voltage Controls	Employ automatic voltage controls for [Assignment: organization-defined critical system components].	PE-9(2)	Not Selected	Functional	Equal	10	Automatic Voltage Controls	PES-07.1	Facility security mechanisms exist to utilize automatic voltage controls for critical system components.																		
PE	PE-10	PE-10	Emergency Shutoff	a. Provide the capability of shutting off power to [Assignment: organization-defined system or individual system components] in emergency situations; b. Place emergency shutoff switches or devices in [Assignment: organization-defined locations] to facilitate access for authorized personnel; and c. Protect emergency shutoff switches or devices from unauthorized activation.	PE-10	Moderate	Functional	Equal	10	Emergency Shutoff	PES-07.2	(1) Placing emergency shutoff switches or devices in close proximity to systems or system components to facilitate safe and easy access for personnel; and		PE-10	PE-10			PE-10	PE-10							PE-10			PE-10
PE	PE-10(01)	PE-10(1)		Withdrawn	PE-10(1)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
PE	PE-11	PE-11	Emergency Power	Provide an uninterruptible power supply to facilitate [Selection (one or more): an orderly shutdown of the system; transition of the system to long-term alternate power] in the event of a primary power source loss.	PE-11	Moderate	Functional	Intersects With	5	Emergency Power	PES-07.3	Facility security mechanisms exist to supply alternate power, capable of maintaining minimally-required operational capability, in the event of an extended loss of the primary power source.		PE-11	PE-11			PE-11	PE-11							PE-11			PE-11
PE	PE-11(01)	PE-11(1)	Emergency Power | Alternate Power Supply — Minimal Operational Capability	Provide an uninterruptible power supply to facilitate [Selection (one or more): the orderly shutdown of all system components; transition of the system to long-term alternate power] in the event of a primary power source loss, that can maintain minimally required operational capability in the event of an extended loss of the primary power source.	PE-11(1)	High	Functional	Intersects With	5	Emergency Power	PES-07.3	Facility security mechanisms exist to supply alternate power, capable of maintaining minimally-required operational capability, in the event of an extended loss of the primary power source.			PE-11(1)				PE-11(01)											PE-11(01)
PE	PE-11(02)	PE-11(2)	Emergency Power | Alternate Power Supply — Self-contained	Provide an uninterruptible power supply to facilitate [Selection (one or more): the orderly shutdown of all system components; transition of the system to long-term alternate power] in the event of a primary power source loss, that is self-contained and not dependent on system resources, to provide power generation. and; Capability of maintaining minimally required operational capability in the event of an extended loss of the primary power source.	PE-11(2)	Not Selected	Functional	Intersects With	5	Emergency Power	PES-07.3	Facility security mechanisms exist to supply alternate power, capable of maintaining minimally-required operational capability, in the event of an extended loss of the primary power source.																		
PE	PE-12	PE-12	Emergency Lighting	Employ and maintain automatic emergency lighting for the system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.	PE-12	Low	Functional	Equal	10	Emergency Lighting	PES-07.4	Facility security mechanisms exist to supply alternate power, capable of maintaining minimally-required operational capability, in the event of an extended loss of the primary power source. In the event of a power outage or disruption and that covers emergency exits and evacuation routes	PE-12	PE-12	PE-12		PE-12	PE-12	PE-12	PE-12						PE-12			PE-12
PE	PE-12(01)	PE-12(1)	Emergency Lighting | Essential Mission and Business Functions	Provide emergency lighting for all areas within the facility supporting essential mission and business functions.	PE-12(1)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
PE	PE-13	PE-13	Fire Protection	Employ and maintain fire detection and suppression systems that are supported by an independent energy source.	PE-13	Low	Functional	Equal	10	Fire Protection	PES-08	Facility security mechanisms exist to utilize and maintain fire suppression and detection devices/systems for the system that are supported by an independent energy source.	PE-13	PE-13	PE-13		PE-13	PE-13	PE-13	PE-13						PE-13	PE-13	PE-13		PE-13
PE	PE-13(01)	PE-13(1)	Fire Protection | Detection Systems — Automatic Activation and Notification	Employ fire detection systems that activate automatically and notify [Assignment: organization-defined personnel or roles] and [Assignment: organization-defined emergency responders] in the event of a fire.	PE-13(1)	Moderate	Functional	Equal	10	Fire Detection Devices	PES-08.1	Facility security mechanisms exist to utilize and maintain fire detection devices/systems that activate automatically and notify organizational personnel and emergency responders in the event of a fire.		PE-13(1)	PE-13(1)			PE-13(01)	PE-13(01)							PE-13(01)			PE-13(01)
PE	PE-13(02)	PE-13(2)	Fire Protection | Suppression Systems — Automatic Activation and Notification	Employ fire suppression systems that activate automatically and notify [Assignment: organization-defined personnel or roles] and [Assignment: organization-defined emergency responders]; and.	PE-13(2)	High	Functional	Intersects With	5	Automatic Fire Suppression	PES-08.3	Facility security mechanisms exist to employ an automatic fire suppression capability for critical systems when the facility is not staffed on a continuous basis.	PE-13(2)	PE-13(2)	PE-13(2)	PE-13(2)	PE-13(02)	PE-13(02)	PE-13(02)	PE-13(02)	PE-13(2)	PE-13(2)	PE-13(2)	PE-13(2)	PE-13(2)			PE-13(02)		PE-13(02)
PE	PE-13(02)	PE-13(2)	Fire Protection | Suppression Systems — Automatic Activation and Notification	Employ fire suppression systems that activate automatically and notify [Assignment: organization-defined personnel or roles] and [Assignment: organization-defined emergency responders]; and.	PE-13(2)	High	Functional	Intersects With	5	Fire Suppression Devices	PES-08.2	Facility security mechanisms exist to utilize fire suppression devices/systems that provide automatic notification of any activation to organizational personnel and emergency responders.	PE-13(2)	PE-13(2)	PE-13(2)	PE-13(2)	PE-13(02)	PE-13(02)	PE-13(02)	PE-13(02)	PE-13(2)	PE-13(2)	PE-13(2)	PE-13(2)	PE-13(2)			PE-13(02)		PE-13(02)
PE	PE-13(03)	PE-13(3)		Withdrawn	PE-13(3)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																PE-13(03)		PE-13(03)
PE	PE-13(04)	PE-13(4)	Fire Protection | Inspections	Ensure the facility where the system resides at [Assignment: organization-defined frequency] has adequate fire suppression and detection systems that are supported by an independent energy source and are inspected by authorized and qualified inspectors and identified deficiencies are resolved within [Assignment: organization-defined time period].	PE-13(4)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
PE	PE-14	PE-14	Environmental Controls	a. Maintain [Selection (one or more): temperature; humidity; pressure; radiation; [Assignment: organization-defined environmental control]] levels within the facility where the system resides at [Assignment: organization-defined acceptable levels]; and b. Monitor environmental control levels [Assignment: organization-defined frequency].	PE-14	Low	Functional	Equal	10	Temperature & Humidity Controls	PES-09	Facility security mechanisms exist to maintain and monitor temperature and humidity levels within the facility.	PE-14	PE-14	PE-14		PE-14	PE-14	PE-14	PE-14						PE-14	PE-14	PE-14		PE-14
PE	PE-14(01)	PE-14(1)	Environmental Controls | Automatic Controls	Employ the following automatic environmental controls in the facility to prevent fluctuations potentially harmful to the system: [Assignment: organization-defined automatic environmental controls].	PE-14(1)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
PE	PE-14(02)	PE-14(2)	Environmental Controls | Monitoring with Alarms and Notifications	Employ environmental control alarms or notification of changes potentially harmful to personnel or equipment to [Assignment: organization-defined personnel or roles] that are both locally and remotely located.	PE-14(2)	Not Selected	Functional	Equal	10	Monitoring with Alarms / Notifications	PES-09.1	Facility security mechanisms exist to trigger an alarm or notification of temperature and humidity changes that be potentially harmful to personnel or equipment.							PE-14(02)									PE-14(02)		PE-14(02)
PE	PE-15	PE-15	Water Damage Protection	Protect the system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.	PE-15	Low	Functional	Equal	10	Water Damage Protection	PES-07.5	Facility security mechanisms exist to protect systems from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly and known to key personnel.	PE-15	PE-15	PE-15		PE-15	PE-15	PE-15	PE-15						PE-15	PE-15	PE-15		PE-15
PE	PE-15(01)	PE-15(1)	Water Damage Protection | Automation Support	Detect the presence of water in the vicinity of [Assignment: organization-defined system components] and alert [Assignment: organization-defined personnel or roles].	PE-15(1)	High	Functional	Equal	10	Automation Support for Water Damage Protection	PES-07.6	Facility security mechanisms exist to detect the presence of water in the vicinity of critical systems and alert organizational personnel or roles.				PE-15(1)				PE-15(01)								PE-15(01)
PE	PE-16	PE-16	Delivery and Removal	Authorize and control [Assignment: organization-defined types of system components] entering and exiting the facility; and b. Maintain records of the system components.	PE-16	Low	Functional	Equal	10	Delivery & Removal	PES-10	Physical access control mechanisms exist to isolate information processing facilities from points such as delivery and loading areas and other points to avoid unauthorized access.	PE-16	PE-16	PE-16		PE-16	PE-16	PE-16	PE-16	PE-16			PE-16	PE-16	PE-16	PE-16	PE-16		PE-16
PE	PE-17	PE-17	Alternate Work Site	a. Determine and document the [Assignment: organization-defined alternate work sites allowed for use by employees]; b. Employ the following controls at alternate work sites: [Assignment: organization-defined controls]; c. Assess the effectiveness of controls at alternate work sites; and d. Provide a means for employees to communicate with information security and privacy personnel in case of incidents.	PE-17	Moderate	Functional	Equal	10	Alternate Work Site	PES-11	Physical security mechanisms exist to utilize appropriate management, operational and technical controls at alternate work sites.			PE-17				PE-17						PE-17	PE-17	PE-17		PE-17
PE	PE-18	PE-18	Location of System Components	Position 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.	PE-18	High	Functional	Intersects With	5	Equipment Siting & Protection	PES-12	Facility security mechanisms exist to locate system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.			PE-18				PE-18			PE-18	PE-18	PE-18					PE-18
PE	PE-18(01)	PE-18(1)		Withdrawn	PE-18(1)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
PE	PE-19	PE-19	Information Leakage	Protect the system from information leakage due to electromagnetic signals emanations.	PE-19	Not Selected	Functional	Equal	10	Information Leakage Due To Electromagnetic Signals Emanations	PES-13	Facility security mechanisms exist to protect the system from information leakage due to electromagnetic signals emanations.																		
PE	PE-19(01)	PE-19(1)	Information Leakage | National Emissions Policies and Procedures	Protect system components, associated data communications, and networks in accordance with national Emissions Security policies and procedures based on the security category or classification of information.	PE-19(1)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
PE	PE-20	PE-20	Asset Monitoring and Tracking	Employ [Assignment: organization-defined asset location technologies] to track and monitor the movement of [Assignment: organization-defined assets] within [Assignment: organization-defined controlled areas].	PE-20	Not Selected	Functional	Equal	10	Asset Monitoring and Tracking	PES-14	Physical security mechanisms exist to employ asset location technologies that track and monitor the location and movement of organization-defined assets within organization-defined controlled areas.											PE-20	PE-20						
PE	PE-21	PE-21	Electromagnetic Pulse Protection	Employ [Assignment: organization-defined measures] against electromagnetic pulse damage for [Assignment: organization-defined systems and system components].	PE-21	Not Selected	Functional	Equal	10	Electromagnetic Pulse (EMP) Protection	PES-15	Physical security mechanisms exist to employ safeguards against Electromagnetic Pulse (EMP) damage for systems and system components.																		
PE	PE-22	PE-22	Component Marking	Mark [Assignment: organization-defined system hardware components] indicating the impact or classification level of the information permitted to be processed, stored, or transmitted by the hardware component.	PE-22	Not Selected	Functional	Intersects With	5	Asset Scope Classification	AST-04.1	Mechanisms exist to determine cybersecurity and data protection control applicability by identifying, assigning and documenting the appropriate asset scope categorization for all Technology Assets, Applications and/or Services (TAAS).	PE-22	PE-22	PE-22	PE-22	PE-22	PE-22	PE-22	PE-22	PE-22	PE-22	PE-22	PE-22	PE-22					
PE	PE-22	PE-22	Component Marking	Mark [Assignment: organization-defined system hardware components] indicating the impact or classification level of the information permitted to be processed, stored, or transmitted by the hardware component.	PE-22	Not Selected	Functional	Intersects With	5	Component Marking	PES-16	Mechanisms exist to mark system hardware components indicating the impact or classification level of the information permitted to be processed, stored or transmitted by the hardware component.	PE-22	PE-22	PE-22	PE-22	PE-22	PE-22	PE-22	PE-22	PE-22	PE-22	PE-22	PE-22	PE-22					
PE	PE-23	PE-23	Facility Location	a. Plan the location or site of the facility where the system resides considering physical and environmental hazards; and b. For existing facilities, consider the physical and environmental hazards in the facility location.	PE-23	Not Selected	Functional	Intersects With	5	Third-Party Processing, Storage and Service Locations	TPM-04.4	Mechanisms exist to restrict the location of information processing/storage based on business requirements.	PE-23	PE-23	PE-23	PE-23	PE-23	PE-23	PE-23	PE-23	PE-23	PE-23	PE-23	PE-23	PE-23					
PE	PE-23	PE-23	Facility Location	a. Plan the location or site of the facility where the system resides considering physical and environmental hazards; and b. For existing facilities, consider the physical and environmental hazards in the facility location.	PE-23	Not Selected	Functional	Intersects With	5	Alternate Processing Site	BCD-09	Mechanisms exist to establish an alternate processing site that provides security measures equivalent to that of the primary site.	PE-23	PE-23	PE-23	PE-23	PE-23	PE-23	PE-23	PE-23	PE-23	PE-23	PE-23	PE-23	PE-23					
PE	PE-23	PE-23	Facility Location	a. Plan the location or site of the facility where the system resides considering physical and environmental hazards; and b. For existing facilities, consider the physical and environmental hazards in the facility location.	PE-23	Not Selected	Functional	Intersects With	5	Alternate Storage Site	BCD-08	Mechanisms exist to establish an alternate storage site that includes both the assets and necessary agreements to permit the storage and recovery of system backup information.	PE-23	PE-23	PE-23	PE-23	PE-23	PE-23	PE-23	PE-23	PE-23	PE-23	PE-23	PE-23	PE-23					
PE	PE-23	PE-23	Facility Location	a. Plan the location or site of the facility where the system resides considering physical and environmental hazards; and b. For existing facilities, consider the physical and environmental hazards in the facility location.	PE-23	Not Selected	Functional	Intersects With	5	Distributed Processing & Storage	SEA-15	Mechanisms exist to distribute processing and storage across multiple physical locations.	PE-23	PE-23	PE-23	PE-23	PE-23	PE-23	PE-23	PE-23	PE-23	PE-23	PE-23	PE-23	PE-23					
PE	PE-23	PE-23	Facility Location	a. Plan the location or site of the facility where the system resides considering physical and environmental hazards; and b. For existing facilities, consider the physical and environmental hazards in the facility location.	PE-23	Not Selected	Functional	Intersects With	5	Equipment Siting & Protection	PES-12	Facility security mechanisms exist to locate system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.	PE-23	PE-23	PE-23	PE-23	PE-23	PE-23	PE-23	PE-23	PE-23	PE-23	PE-23	PE-23	PE-23					
PE	PE-23	PE-23	Facility Location	a. Plan the location or site of the facility where the system resides considering physical and environmental hazards; and b. For existing facilities, consider the physical and environmental hazards in the facility location.	PE-23	Not Selected	Functional	Intersects With	5	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	PE-23	PE-23	PE-23	PE-23	PE-23	PE-23	PE-23	PE-23	PE-23	PE-23	PE-23	PE-23	PE-23					
PL	PL-01	PL-1	Policy and Procedures	Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: [Assignment: organization-defined security and privacy policies]; and [Assignment: organization-defined personnel or roles] with the [Assignment: organization-defined frequency]:	PL-1	Low	Functional	Subset Of	10	Cybersecurity & Data Protection Governance Program	PRM-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection-related resource planning controls that define a viable plan for achieving cybersecurity and data protection objectives.	PL-1	PL-1	PL-1	PL-1	PL-01

Family	Sorting Control #	Focal Document Element	Focal Document Element Name	Focal Document Element Description	NIST SP 800-53 R5.2	Security Control Baseline	Set Theory Relationship Mapping (STRM) Rationale	Relationship	Strength of Relationship	Reference Document Element	Reference Document Name	Reference Document Element Description	NIST SP 800-53 R5.2 Baselines Low	Mod	High	Privacy	FedRAMP R5 Low	Mod	High	LI-SaaS	CSCRM Baseline	NIST SP 800-161 R1 Down	Level 1	Level 2	Level 3	GovRAMP Low	Low+	Moderate	Core	High (FedRAMP Rev 5)
PL	PL-09	PL-9	Central Management	Centrally manage [Assignment: organization-defined controls and related processes]	PL-9	Not Selected	Functional	Intersects With	5	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity and	PL-9	PL-9	PL-9	PL-9	PL-09	PL-09	PL-09	PL-09	PL-9	PL-9	PL-9	PL-9	PL-9					
PL	PL-09	PL-9	Central Management	Centrally manage [Assignment: organization-defined controls and related processes]	PL-9	Not Selected	Functional	Intersects With	5	Centralized Management of Antimalware Technologies	END-04.3	Mechanisms exist to centrally-manage antimalware technologies.	PL-9	PL-9	PL-9	PL-9	PL-09	PL-09	PL-09	PL-09	PL-9	PL-9	PL-9	PL-9	PL-9					
PL	PL-09	PL-9	Central Management	Centrally manage [Assignment: organization-defined controls and related processes]	PL-9	Not Selected	Functional	Intersects With	5	Central Management	END-08.1	Mechanisms exist to centrally-manage anti-phishing and spam protection technologies.	PL-9	PL-9	PL-9	PL-9	PL-09	PL-09	PL-09	PL-09	PL-9	PL-9	PL-9	PL-9	PL-9					
PL	PL-09	PL-9	Central Management	Centrally manage [Assignment: organization-defined controls and related processes]	PL-9	Not Selected	Functional	Intersects With	5	Centralized Management of Planned Audit Record Content	MON-03.6	Mechanisms exist to centrally manage and configure the content required to be captured in audit records generated by organization-defined system components.	PL-9	PL-9	PL-9	PL-9	PL-09	PL-09	PL-09	PL-09	PL-9	PL-9	PL-9	PL-9	PL-9					
PL	PL-10	PL-10	Baseline Selection	Select a control baseline for the system.	PL-10	Low	Functional	Equal	10	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system	PL-10	PL-10	PL-10		PL-10	PL-10	PL-10	PL-10	PL-10			PL-10	PL-10					
PL	PL-11	PL-11	Baseline Tailoring	Tailor the selected control baseline by applying specified tailoring actions	PL-11	Low	Functional	Equal	10	Baseline Tailoring	CFG-02.9	(1) Mission / business functions; (2) Operational environment;	PL-11	PL-11	PL-11		PL-11	PL-11	PL-11	PL-11										
PM	PM-01	PM-1	Information Security Program Plan	Develop and update [Assignment: organization-defined frequency] an information security program plan for the organization; and	PM-1	Not Associated	Functional	Subset Of	10	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls.	PM-1	PM-1	PM-1	PM-1	PM-01	PM-01	PM-01	PM-01	PM-1	PM-1	PM-1	PM-1	PM-1					
PM	PM-01	PM-1	Information Security Program Plan	Develop and update [Assignment: organization-defined frequency] an information security program plan for the organization; and	PM-1	Not Associated	Functional	Intersects With	5	Cybersecurity & Data Protection Governance Program	GOV-03	Mechanisms exist to maintain a documented cybersecurity and data protection governance program that includes standards and procedures, at planned intervals or if significant changes occur to ensure their	PM-1	PM-1	PM-1	PM-1	PM-01	PM-01	PM-01	PM-01	PM-1	PM-1	PM-1	PM-1	PM-1					
PM	PM-01	PM-1	Information Security Program Plan	Develop and update [Assignment: organization-defined frequency] an information security program plan for the organization; and	PM-1	Not Associated	Functional	Intersects With	5	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	PM-1	PM-1	PM-1	PM-1	PM-01	PM-01	PM-01	PM-01	PM-1	PM-1	PM-1	PM-1	PM-1					
PM	PM-02	PM-2	Information Security Program Leadership Role	Appoint [Assignment: organization-defined information security leadership role] to coordinate, develop, implement, and maintain an organization-wide information security program.	PM-2	Not Associated	Functional	Intersects With	5	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity and							PM-2				PM-2							
PM	PM-03	PM-3	Information Security and Privacy Resources	Include the resources needed to implement the information security and privacy programs in capital planning and documentation required for addressing information security and privacy programs in capital planning and	PM-3	Not Associated	Functional	Equal	10	Cybersecurity & Data Protection Resource Management	PRM-02	Mechanisms exist to identify and allocate resources for management, operational, technical and data privacy requirements within business process planning for projects / initiatives.				PM-3							PM-3							
PM	PM-04	PM-4	Plan of Action and Milestones Process	Implement a process to ensure that plans of action and milestones for the information security, privacy, and supply chain risk management programs and associated organizational systems: a. Are developed and maintained; b. Document the remedial information security, privacy, and supply chain risk management actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and c. Are reported in accordance with established reporting requirements.	PM-4	Not Associated	Functional	Intersects With	5	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	PM-4	PM-4	PM-4	PM-4	PM-04	PM-04	PM-04	PM-04	PM-4	PM-4	PM-4	PM-4	PM-4					
PM	PM-04	PM-4	Plan of Action and Milestones Process	Implement a process to ensure that plans of action and milestones for the information security, privacy, and supply chain risk management programs and associated organizational systems: a. Are developed and maintained; b. Document the remedial information security, privacy, and supply chain risk management actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and c. Are reported in accordance with established reporting requirements.	PM-4	Not Associated	Functional	Intersects With	5	Plan of Action & Milestones (POA&M)	IAO-05	Mechanisms exist to ensure that plans of action and milestones (POA&M), or similar risk document, are maintained and used to track and remediate cybersecurity and data privacy control weaknesses.	PM-4	PM-4	PM-4	PM-4	PM-04	PM-04	PM-04	PM-04	PM-4	PM-4	PM-4	PM-4	PM-4					
PM	PM-05	PM-5	System Inventory	Develop and update [Assignment: organization-defined frequency] an inventory of organizational systems.	PM-5	Not Associated	Functional	Intersects With	5	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	PM-5	PM-5	PM-5	PM-5	PM-05	PM-05	PM-05	PM-05	PM-5	PM-5	PM-5	PM-5	PM-5					
PM	PM-05	PM-5	System Inventory	Develop and update [Assignment: organization-defined frequency] an inventory of organizational systems.	PM-5	Not Associated	Functional	Intersects With	5	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TASD) that:	PM-5	PM-5	PM-5	PM-5	PM-05	PM-05	PM-05	PM-05	PM-5	PM-5	PM-5	PM-5	PM-5					
PM	PM-05(01)	PM-5(1)	System Inventory | Inventory of Personally Identifiable Information	Establish, maintain, and update [Assignment: organization-defined frequency] an inventory of all systems, applications, and projects that process the authorized processing of personally identifiable information.	PM-5(1)	Not Associated	Functional	Intersects With	5	Inventory of Personal Data (PD)	PRI-05.5	Mechanisms exist to establish and maintain a current inventory of all Technology Assets, Applications and/or Services (TASS) that collect, receive, process, store, transmit, update and/or share Personal	PM-5(1)	PM-5(1)	PM-5(1)	PM-5(1)	PM-05(01)	PM-05(01)	PM-05(01)	PM-05(01)	PM-5(1)	PM-5(1)	PM-5(1)	PM-5(1)	PM-5(1)					
PM	PM-05(01)	PM-5(1)	System Inventory | Inventory of Personally Identifiable Information	Establish, maintain, and update [Assignment: organization-defined frequency] an inventory of all systems, applications, and projects that process the authorized processing of personally identifiable information.	PM-5(1)	Not Associated	Functional	Intersects With	5	Personal Data Inventory Automation Support	PRI-05.6	Automated mechanisms exist to determine if Personal Data (PD) is maintained in electronic form.	PM-5(1)	PM-5(1)	PM-5(1)	PM-5(1)	PM-05(01)	PM-05(01)	PM-05(01)	PM-05(01)	PM-5(1)	PM-5(1)	PM-5(1)	PM-5(1)	PM-5(1)					
PM	PM-06	PM-6	Measures of Performance	Develop, monitor, and report on the results of information security and privacy measures of performance.	PM-6	Not Associated	Functional	Intersects With	5	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity and	PM-6	PM-6	PM-6	PM-6	PM-06	PM-06	PM-06	PM-06	PM-6	PM-6	PM-6	PM-6	PM-6					
PM	PM-06	PM-6	Measures of Performance	Develop, monitor, and report on the results of information security and privacy measures of performance.	PM-6	Not Associated	Functional	Intersects With	5	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity and data protection program measures of performance.	PM-6	PM-6	PM-6	PM-6	PM-06	PM-06	PM-06	PM-06	PM-6	PM-6	PM-6	PM-6	PM-6					
PM	PM-07	PM-7	Enterprise Architecture	Develop and maintain an enterprise architecture with consideration for information security, privacy, and the resulting risk to organizational operations and assets, individuals, other organizations, and the Nation that describes the architectural decisions that are intended to be implemented centrally, across organizational segments, and at the system level.	PM-7	Not Associated	Functional	Intersects With	5	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry practices, with consideration for cybersecurity and data protection principles that addresses risk to				PM-7							PM-7							
PM	PM-07(01)	PM-7(1)	Enterprise Architecture | Offloading	Offload [Assignment: organization-defined non-essential functions or services] to other systems, system components, or an external provider.	PM-7(1)	Not Associated	Functional	Equal	10	Outsourcing Non-Essential Functions or Services	SEA-02.2	Mechanisms exist to identify non-essential functions or non-security data in the process of being transferred to external service providers and align with the organization's enterprise architecture and security																		
PM	PM-08	PM-8	Critical Infrastructure Plan	Address information security, privacy, and supply chain risk management in the development, documentation, and updating of a critical infrastructure and key resources protection plan.	PM-8	Not Associated	Functional	Intersects With	5	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure Resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan	PM-8	PM-8	PM-8	PM-8	PM-08	PM-08	PM-08	PM-08	PM-8	PM-8	PM-8	PM-8	PM-8					
PM	PM-08	PM-8	Critical Infrastructure Plan	Address information security, privacy, and supply chain risk management in the development, documentation, and updating of a critical infrastructure and key resources protection plan.	PM-8	Not Associated	Functional	Intersects With	5	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	PM-8	PM-8	PM-8	PM-8	PM-08	PM-08	PM-08	PM-08	PM-8	PM-8	PM-8	PM-8	PM-8					
PM	PM-09	PM-9	Risk Management Strategy	Develop a comprehensive strategy to manage: a. Security risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of systems; and b. Privacy risk to individuals resulting from the authorized processing of personally identifiable information; c. Review and update the risk management strategy [Assignment: organization-defined frequency] or as required, to address organizational changes; and d. Establish organizational risk tolerance and monitor risk measures across the organization.	PM-9	Not Associated	Functional	Equal	10	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.				PM-9							PM-9							
PM	PM-10	PM-10	Authorization Process	Manage the security and privacy state of organizational systems and the environments in which those systems operate through authorization processes; b. Designate individuals to fulfill specific roles and responsibilities within the organizational risk management process; and c. Integrate the authorization processes into an organization-wide risk management program.	PM-10	Not Associated	Functional	Equal	10	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection assessment and authorization controls.				PM-10							PM-10	PM-10						
PM	PM-11	PM-11	Mission and Business Process Definition	Define organizational mission and business processes with consideration for information security and privacy and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and b. Determine information protection and personally identifiable information processing needs arising from the defined mission and business processes; and c. Review and revise the mission and business processes [Assignment: organization-defined frequency].	PM-11	Not Associated	Functional	Equal	10	Business Process Definition	PRM-06	(1) The resulting risk to organizational operations, assets, individuals and other organizations; and				PM-11							PM-11	PM-11	PM-11					
PM	PM-12	PM-12	Insider Threat Program	Implement an insider threat program that includes a cross-discipline insider threat incident handling team.	PM-12	Not Associated	Functional	Equal	10	Insider Threat Program	THR-04	Mechanisms exist to implement an insider threat program that includes a cross-discipline insider threat incident handling team.											PM-12	PM-12	PM-12					
PM	PM-13	PM-13	Security and Privacy Workforce	Establish a security and privacy workforce development and improvement program.	PM-13	Not Associated	Functional	Intersects With	5	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	PM-13	PM-13	PM-13	PM-13	PM-13	PM-13	PM-13	PM-13	PM-13	PM-13	PM-13	PM-13	PM-13					
PM	PM-13	PM-13	Security and Privacy Workforce	Establish a security and privacy workforce development and improvement program.	PM-13	Not Associated	Functional	Intersects With	5	Cybersecurity & Data Protection-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	PM-13	PM-13	PM-13	PM-13	PM-13	PM-13	PM-13	PM-13	PM-13	PM-13	PM-13	PM-13	PM-13					
PM	PM-14	PM-14	Testing, Training, and Monitoring	Implement a process for ensuring that organizational plans for conducting [Assignment: organization-defined security and privacy assessments, privacy impact assessments, and other reviews and testing] are developed and maintained; and2. Continue to be executed; and b. Implement a process for ensuring that organizational plans for conducting [Assignment: organization-defined security and privacy assessments, privacy impact assessments, and other reviews and testing] are developed and maintained; and2. Continue to be executed; and3. Reviews testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.	PM-14	Not Associated	Functional	Intersects With	5	Testing, Training & Monitoring	PRI-08	Mechanisms exist to conduct cybersecurity and data protection testing, training and monitoring activities	PM-14	PM-14	PM-14	PM-14	PM-14	PM-14	PM-14	PM-14	PM-14	PM-14	PM-14	PM-14	PM-14					
PM	PM-14	PM-14	Testing, Training, and Monitoring	Implement a process for ensuring that organizational plans for conducting [Assignment: organization-defined security and privacy assessments, privacy impact assessments, and other reviews and testing] are developed and maintained; and2. Continue to be executed; and b. Implement a process for ensuring that organizational plans for conducting [Assignment: organization-defined security and privacy assessments, privacy impact assessments, and other reviews and testing] are developed and maintained; and2. Continue to be executed; and3. Reviews testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.	PM-14	Not Associated	Functional	Intersects With	5	Cybersecurity & Data Protection Controls Oversight	CPL-02	Mechanisms exist to provide a cybersecurity and data protection controls oversight function that reports to the organization's executive leadership.	PM-14	PM-14	PM-14	PM-14	PM-14	PM-14	PM-14	PM-14	PM-14	PM-14	PM-14	PM-14	PM-14					
PM	PM-15	PM-15	Security and Privacy Groups and Associations	Establish and institutionalize contact with selected groups and associations within the security and privacy communities: a. To facilitate ongoing security and privacy education and training for organizational personnel; b. To maintain currency with recommended security and privacy practices, techniques, and technologies; and c. To share current security and privacy information, including threats, vulnerabilities, and incidents.	PM-15	Not Associated	Functional	Intersects With	5	Threat Intelligence Feeds Program	THR-01	Mechanisms exist to establish an organization-wide threat intelligence program.	PM-15	PM-15	PM-15	PM-15	PM-15	PM-15	PM-15	PM-15	PM-15	PM-15	PM-15	PM-15	PM-15					
PM	PM-15	PM-15	Security and Privacy Groups and Associations	Establish and institutionalize contact with selected groups and associations within the security and privacy communities: a. To facilitate ongoing security and privacy education and training for organizational personnel; b. To maintain currency with recommended security and privacy practices, techniques, and technologies; and c. To share current security and privacy information, including threats, vulnerabilities, and incidents.	PM-15	Not Associated	Functional	Intersects With	5	Contacts With Groups & Associations	GOV-07	(2) Maintain currency with recommended cybersecurity and data protection practices, techniques and	PM-15	PM-15	PM-15	PM-15	PM-15	PM-15	PM-15	PM-15	PM-15	PM-15	PM-15	PM-15	PM-15					
PM	PM-16	PM-16	Threat Awareness Program	Implement a threat awareness program that includes a cross-organization information-sharing capability for threat intelligence.	PM-16	Not Associated	Functional	Intersects With	5	Threat Intelligence Feeds Program	THR-01	Mechanisms exist to establish an organization-wide threat intelligence program.											PM-16	PM-16						
PM	PM-16(01)	PM-16(1)	Threat Awareness Program | Automated Means for Sharing Threat Intelligence	Employ automated mechanisms to maximize the effectiveness of sharing threat intelligence information.	PM-16(1)	Not Associated	Functional	Intersects With	5	Threat Intelligence Feeds Feeds	THR-03	Mechanisms exist to maintain situational awareness of evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the																		
PM	PM-17	PM-17	Protecting Controlled Unclassified Information on External Systems	Establish policy and procedures to ensure that requirements for the protection of controlled unclassified information processed, stored or transmitted on external systems, are implemented in accordance with applicable laws, executive orders, directives, policies, regulations, standards, and guidance.	PM-17	Not Associated	Functional	Equal	10	Protecting Sensitive Data on External Systems	DCH-13.3	Mechanisms exist to ensure that the requirements for the protection of sensitive information processed, stored or transmitted on external Technology Assets, Applications and/or Services (TAAS), are				PM-17									PM-17					
PM	PM-18	PM-18	Privacy Program Plan	Develop and disseminate an organization-wide privacy program plan that provides an overview of the agency's privacy program, and: a. Includes a description of the structure of the privacy program and the resources dedicated to the privacy program; b. Provides an overview of the requirements for the privacy program and a description of the privacy controls in place or planned for meeting those requirements; c. Includes the role of the senior agency official for privacy and the identification and assignment of roles of other privacy officials and staff and their responsibilities; d. Describes management commitment, compliance, and strategic goals and objectives of the privacy program; e. Reflects coordination among organizational entities responsible for the various aspects of privacy; and f. Is approved by a senior official with responsibility and accountability for the privacy risk being incurred to organizational operations and assets, individuals, other organizations, and the Nation; and b. Update the plan [Assignment: organization-defined frequency] and to address changes in federal privacy laws and policy and organizational changes and problems identified during plan implementation or privacy control assessments.	PM-18	Not Associated	Functional	Equal	10	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data privacy controls.				PM-18					PM-18	PM-18	PM-18					
PM	PM-19	PM-19	Privacy Program Leadership Role	Appoint a senior agency official for privacy with the authority, mission, accountability, and resources to coordinate, develop, and implement, applicable data privacy practices within the organization and to ensure that the organization considers privacy issues in all of its functions that require the collection, use, maintenance, sharing, or disposal of personally identifiable information (PII).	PM-19	Not Associated	Functional	Equal	10	Chief Privacy Officer (CPO)	PRI-01.1	Mechanisms exist to appoint a Chief Privacy Officer (CPO), or similar role, with the authority, mission, accountability and resources to coordinate, develop and implement, applicable data privacy				PM-19							PM-19							
PM	PM-20	PM-20	Dissemination of Privacy Program Information	Maintain a central resource webpage on the organization's principal public website that serves as a central source of information about the organization's privacy program and that: a. Ensures that the public has access to information about organizational privacy activities and can communicate with its senior agency official for privacy; b. Ensures that organizational privacy practices and reports are easily accessible for review; and c. Ensures that organizational privacy reports are available in a format that allows the reader to retrieve, display, and search its contents.	PM-20	Not Associated	Functional	Equal	10	Dissemination of Data Privacy Program Information	PRI-01.3	(2) Ensure that organizational data privacy practices are publicly available through organizational websites or document repositories;				PM-20							PM-20							
PM	PM-20(01)	PM-20(1)	Dissemination of Privacy Program Information | Privacy Policies on Websites, Applications, and Digital Services	Develop and post privacy policies on all external-facing websites, mobile applications, and other digital services, that: a. Are written in plain language and organized in a way that is easy to understand and navigate; b. Provide information needed by the public to make an informed decision about whether and how to interact with the organization; and c. Are updated whenever the organization makes a substantive change to the practices it describes and includes a time_restricted_data that indicates when the last update was made.	PM-20(1)	Not Associated	Functional	Intersects With	5	Data Privacy Notice	PRI-02	Personal Data (PD) processing in plain language that meets all legal obligations;				PM-20(1)														
PM	PM-21	PM-21	Accounting of Disclosures	Develop and maintain an accurate accounting of disclosures of personally identifiable information, including personally identifiable information disclosed under a matching program, and disclosures made to parties to which personally identifiable information has been released (including the name, position title, and mailing address of the person to whom the personally identifiable information was released).	PM-21	Not Associated	Functional	Intersects With	5	Accounting of Disclosures	PRI-14.1	Mechanisms exist to maintain an accounting of disclosures available to the person named in the record.				PM-21							PM-21	PM-21						
PM	PM-22	PM-22	Personally Identifiable Information Quality Management	Develop and document organization-wide policies and procedures for: a. Reviewing for the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information lifecycle; b. Correcting or deleting inaccurate or outdated personally identifiable information; c. Disseminating notice of	PM-22	Not Associated	Functional	Intersects With	5	Data Quality Management	PRI-10	Mechanisms exist to manage the quality, utility, objectivity, integrity and impact determination and de-identification of sensitive/regulated data across the information lifecycle.	PM-22	PM-22	PM-22	PM-22	PM-22	PM-22	PM-22	PM-22	PM-22	PM-22	PM-22	PM-22	PM-22					
PM	PM-22	PM-22	Personally Identifiable Information Quality Management	Develop and document organization-wide policies and procedures for: a. Reviewing for the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information lifecycle; b. Correcting or deleting inaccurate or outdated personally identifiable information; c. Disseminating notice of	PM-22	Not Associated	Functional	Intersects With	5	Data Quality Operations	DCH-22	Mechanisms exist to check the accuracy, relevance, timeliness, impact, completeness and de-identification of information	PM-22	PM-22	PM-22	PM-22	PM-22	PM-22	PM-22	PM-22	PM-22	PM-22	PM-22	PM-22	PM-22					
PM	PM-23	PM-23	Data Governance Body	Establish a Data Governance Body consisting of [Assignment: organization-defined roles] with [Assignment: organization-defined responsibilities].	PM-23	Not Associated	Functional	Intersects With	5	Data Management Board	PRI-13	Mechanisms exist to establish a written charter for a Data Management Board (DMB) and assigned organization-defined roles to the DMB.	PM-23	PM-23	PM-23	PM-23	PM-23	PM-23	PM-23	PM-23	PM-23	PM-23	PM-23	PM-23	PM-23					
PM	PM-23	PM-23	Data Governance Body	Establish a Data Governance Body consisting of [Assignment: organization-defined roles] with [Assignment: organization-defined responsibilities].	PM-23	Not Associated	Functional	Intersects With	5	Data Quality Management	PRI-10	Mechanisms exist to manage the quality, utility, objectivity, integrity and impact determination and de-identification of sensitive/regulated data across the information lifecycle.	PM-23	PM-23	PM-23	PM-23	PM-23	PM-23	PM-23	PM-23	PM-23	PM-23	PM-23	PM-23	PM-23					
PM	PM-23	PM-23	Data Governance Body	Establish a Data Governance Body consisting of [Assignment: organization-defined roles] with [Assignment: organization-defined responsibilities].	PM-23	Not Associated	Functional	Intersects With	5	Data Governance	GOV-10	Mechanisms exist to govern data, documenting the applicable data specification, standards, and procedures so that sensitive/regulated data is effectively managed and maintained in accordance with	PM-23	PM-23	PM-23	PM-23	PM-23	PM-23	PM-23	PM-23	PM-23	PM-23	PM-23	PM-23	PM-23					
PM	PM-24	PM-24	Data Integrity Board	Establish a Data Integrity Board to: a. Review proposals to conduct or participate in a matching program; and b. Conduct an annual review of all matching programs in which the agency has participated.	PM-24	Not Associated	Functional	Intersects With	5	Data Governance	GOV-10	Mechanisms exist to govern data, documenting the applicable data specification, standards and procedures so that sensitive/regulated data is effectively managed and maintained in accordance with	PM-24	PM-24	PM-24	PM-24	PM-24	PM-24	PM-24	PM-24	PM-24	PM-24	PM-24	PM-24	PM-24					
PM	PM-24	PM-24	Data Integrity Board	Establish a Data Integrity Board to: a. Review proposals to conduct or participate in a matching program; and b. Conduct an annual review of all matching programs in which the agency has participated.	PM-24	Not Associated	Functional	Intersects With	5	Data Management Board	PRI-13	Mechanisms exist to establish a written charter for a Data Management Board (DMB) and assigned organization-defined roles to the DMB.	PM-24	PM-24	PM-24	PM-24	PM-24	PM-24	PM-24	PM-24	PM-24	PM-24	PM-24	PM-24	PM-24					
PM	PM-24	PM-24	Data Integrity Board	Establish a Data Integrity Board to: a. Review proposals to conduct or participate in a matching program; and b. Conduct an annual review of all matching programs in which the agency has participated.	PM-24	Not Associated	Functional	Intersects With	5	Data Quality Management	PRI-10	Mechanisms exist to manage the quality, utility, objectivity, integrity and impact determination and de-identification of sensitive/regulated data across the information lifecycle.	PM-24	PM-24	PM-24	PM-24	PM-24	PM-24	PM-24	PM-24	PM-24	PM-24	PM-24	PM-24	PM-24					
PM	PM-24	PM-24	Data Integrity Board	Establish a Data Integrity Board to: a. Review proposals to conduct or participate in a matching program; and b. Conduct an annual review of all matching programs in which the agency has participated.	PM-24	Not Associated	Functional	Intersects With	5	Personal Data Accuracy & Integrity	PRI-05.2	Mechanisms exist to confirm the accuracy and relevance of Personal Data (PD) throughout the information lifecycle.	PM-24	PM-24	PM-24	PM-24	PM-24	PM-24	PM-24	PM-24	PM-24	PM-24	PM-24	PM-24	PM-24					
PM	PM-24	PM-24	Data Integrity Board	Establish a Data Integrity Board to: a. Review proposals to conduct or participate in a matching program; and b. Conduct an annual review of all matching programs in which the agency has participated.	PM-24	Not Associated	Functional	Intersects With	5	Computer Matching Agreements (CMA)	PRI-02.3	Mechanisms exist to publish Computer Matching Agreements (CMA) on the public website of the organization.	PM-24	PM-24	PM-24	PM-24	PM-24	PM-24	PM-24	PM-24	PM-24	PM-24	PM-24	PM-24	PM-24					
PM	PM-24	PM-24	Data Integrity Board	Establish a Data Integrity Board to: a. Review proposals to conduct or participate in a matching program; and b. Conduct an annual review of all matching programs in which the agency has participated.	PM-24	Not Associated	Functional	Intersects With	5	Automated Data Management Processes	PRI-02.2	Automated mechanisms exist to adjust data that is able to be collected, created, used, disseminated, maintained, retained and/or disclosed, based on updated data subject authorization(s).	PM-24	PM-24	PM-24	PM-24	PM-24	PM-24	PM-24	PM-24	PM-24	PM-24	PM-24	PM-24	PM-24					
PM	PM-25	PM-25	Minimization of Personally Identifiable Information Used in Testing, Training, and Research	Limit or minimize the use of personally identifiable information to [Assignment: organization-defined conditions].	PM-25	Not Associated	Functional	Intersects With	5	Usage Restrictions of Sensitive Personal Data	PRI-05.4	Mechanisms exist to restrict the use of Personal Data (PD) to only the authorized purpose(s) consistent with applicable laws, regulations and in data privacy notices.	PM-25	PM-25	PM-25	PM-25	PM-25	PM-25	PM-25	PM-25	PM-25	PM-25	PM-25	PM-25	PM-25					
PM	PM-25	PM-25	Minimization of Personally Identifiable Information Used in Testing, Training, and Research	Limit or minimize the use of personally identifiable information to [Assignment: organization-defined conditions].	PM-25	Not Associated	Functional	Intersects With	5	Collection Minimization	END-13.3	Mechanisms exist to utilize sensors that are configured to minimize the collection of information about individuals.	PM-25	PM-25	PM-25	PM-25	PM-25	PM-25	PM-25	PM-25	PM-25	PM-25	PM-25	PM-25	PM-25					
PM	PM-25	PM-25	Minimization of Personally Identifiable Information Used in Testing, Training, and Research	Limit or minimize the use of personally identifiable information to [Assignment: organization-defined conditions].	PM-25	Not Associated	Functional	Intersects With	5	Minimize Visitor Personal Data (PD)	PES-06.5	Mechanisms exist to minimize the collection of Personal Data (PD) contained in visitor access records.	PM-25	PM-25	PM-25	PM-25	PM-25	PM-25	PM-25	PM-25	PM-25	PM-25	PM-25	PM-25	PM-25					
PM	PM-25	PM-25	Minimization of Personally Identifiable Information Used in Testing, Training, and Research	Limit or minimize the use of personally identifiable information to [Assignment: organization-defined conditions].	PM-25	Not Associated	Functional	Intersects With	5	Internal Use of Personal Data For Testing, Training and Research	PRI-05.1	(1) Takes measures to limit or minimize the amount of PD used for internal testing, training and research purposes; and	PM-25	PM-25	PM-25	PM-25	PM-25	PM-25	PM-25	PM-25	PM-25	PM-25	PM-25	PM-25	PM-25					
PM	PM-25	PM-25	Minimization of Personally Identifiable Information Used in Testing, Training, and Research	Limit or minimize the use of personally identifiable information to [Assignment: organization-defined conditions].	PM-25	Not Associated	Functional	Intersects With	5	Limit Sensitive / Regulated Data In Testing, Training & Research	DCH-18.2	Mechanisms exist to minimize the use of sensitive/regulated data for research, testing, or training, in accordance with authorized, legitimate business practices.	PM-25	PM-25	PM-25	PM-25	PM-25	PM-25	PM-25	PM-25	PM-25	PM-25	PM-25	PM-25	PM-25					
PM	PM-26	PM-26	Complaint Management	Implement a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices that includes mechanisms to ensure that each complaint is reviewed and addressed within [Assignment: organization-defined time period]; b. Includes mechanisms to ensure that each complaint is reviewed and addressed within [Assignment: organization-defined time period]; and c. Provides mechanisms for appropriate	PM-26	Not Associated	Functional	Intersects With	5	User Feedback Management	PRI-06.4	Mechanisms exist to implement a process for receiving and responding to complaints, concerns or questions from data subjects about the organizational data privacy practices	PM-26	PM-26	PM-26	PM-26	PM-26	PM-26	PM-26	PM-26	PM-26	PM-26	PM-26	PM-26	PM-26					
PM	PM-26	PM-26	Complaint Management	Implement a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices that includes mechanisms to ensure that each complaint is reviewed and addressed within [Assignment: organization-defined time period]; b. Includes mechanisms to ensure that each complaint is reviewed and addressed within [Assignment: organization-defined time period]; and c. Provides mechanisms for appropriate	PM-26	Not Associated	Functional	Intersects With	5	Appeal Adverse Decision	PRI-06.3	Mechanisms exist to establish procedures to allow individuals to appeal an adverse decision and have incorrect information amended.	PM-26	PM-26	PM-26	PM-26	PM-26	PM-26	PM-26	PM-26	PM-26	PM-26	PM-26	PM-26	PM-26					
PM	PM-27	PM-27	Privacy Reporting	Develop [Assignment: organization-defined privacy re

Family	Sorting Control #	Focal Document Element	Focal Document Element Name	Focal Document Element Description	NIST SP 800-53 R5.2	Security Control Baseline	Set Theory Relationship Mapping (STRM) Rationale	Set Theory Relationship Mapping (STRM) Relationship	Set Theory Relationship Mapping (STRM) Strength of Relationship	Reference Document Element	Reference Document Element Name	Reference Document Element Description	NIST SP 800-53 R5.2 Baselines Low	Mod	High	Privacy	FedRAMP R5 Low	Mod	High	LI-SaaS	CS-CRM Baseline	NIST SP 800-161 R1 Down	Level 1	Level 2	Level 3	GovRAMP Low	Low+	Moderate	Core	High (FedRAMP Rev. 5)
PT	PT-01	PT-1	Policy and Procedures	processing and transparency policy and the associated personally identifiable information processing and	PT-1	Not Selected	Functional	Subset Of	10	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity and data	PT-1	PT-1	PT-1	PT-1	PT-01	PT-01	PT-01	PT-01	PT-1	PT-1	PT-1	PT-1	PT-1					
PT	PT-02	PT-2	Authority to Process Personally Identifiable Information	personally identifiable information; and b. Restrict the	PT-2	Not Selected	Functional	Intersects With	5	Authority To Collect, Use, Maintain & Share Personal Data	PRI-04.1	maintenance and sharing of Personal Data (PD), either generally or in support of a specific program or	PT-2	PT-2	PT-2	PT-2	PT-02	PT-02	PT-02	PT-02	PT-2	PT-2	PT-2	PT-2	PT-2					
PT	PT-02	PT-2	Authority to Process Personally Identifiable Information	personally identifiable information; and b. Restrict the	PT-2	Not Selected	Functional	Intersects With	5	Internal Use Of Personal Data For Testing, Training and Research	PRI-05.1	(1) Takes measures to limit or minimize the amount of PD used for internal testing, training and research purposes; and	PT-2	PT-2	PT-2	PT-2	PT-02	PT-02	PT-02	PT-02	PT-2	PT-2	PT-2	PT-2	PT-2					
PT	PT-02	PT-2	Authority to Process Personally Identifiable Information	personally identifiable information; and b. Restrict the	PT-2	Not Selected	Functional	Intersects With	5	Usage Restrictions of Sensitive Personal Data	PRI-05.4	Mechanisms exist to restrict the use of Personal Data (PD) to only the authorized purpose(s) consistent with applicable laws, regulations and in data privacy notices.	PT-2	PT-2	PT-2	PT-2	PT-02	PT-02	PT-02	PT-02	PT-2	PT-2	PT-2	PT-2	PT-2					
PT	PT-02	PT-2	Authority to Process Personally Identifiable Information	personally identifiable information; and b. Restrict the	PT-2	Not Selected	Functional	Intersects With	5	Restrict Collection To Identified Purpose	PRI-04	notice and includes protections against collecting PD from minors without appropriate parental, or legal	PT-2	PT-2	PT-2	PT-2	PT-02	PT-02	PT-02	PT-02	PT-2	PT-2	PT-2	PT-2	PT-2					
PT	PT-02(01)	PT-2(1)	Authority to Process Personally Identifiable Information | Data Tagging	Authority to Process Personally Identifiable Information | Data Tagging	PT-2(1)	Not Selected	Functional	Equal	10	Data Tags	DCH-22.2	Mechanisms exist to utilize data tags to automate tracking of sensitive/regulated data across the information lifecycle.																		
PT	PT-02(02)	PT-2(2)	Authority to Process Personally Identifiable Information | Automation	Authority to Process Personally Identifiable Information | Automation	PT-2(2)	Not Selected	Functional	Intersects With	5	Automated Data Management Processes	PRI-02.2	Automated mechanisms exist to adjust data that is able to be collected, created, used, disseminated, maintained, retained and/or disclosed, based on updated data subject authorization(s).																		
PT	PT-03	PT-3	Personally Identifiable Information Processing Purposes	processing] of personally identifiable information to only	PT-3	Not Selected	Functional	Intersects With	5	Internal Use of Personal Data For Testing, Training and Research	PRI-05.1	(1) Takes measures to limit or minimize the amount of PD used for internal testing, training and research purposes; and	PT-3	PT-3	PT-3	PT-3	PT-03	PT-03	PT-03	PT-03	PT-3	PT-3	PT-3	PT-3	PT-3					
PT	PT-03	PT-3	Personally Identifiable Information Processing Purposes	processing] of personally identifiable information to only	PT-3	Not Selected	Functional	Intersects With	5	Purpose Specification	PRI-02.1	Mechanisms exist to identify and document the purpose(s) for which Personal Data (PD) is collected, used, maintained and shared in its data privacy notices.	PT-3	PT-3	PT-3	PT-3	PT-03	PT-03	PT-03	PT-03	PT-3	PT-3	PT-3	PT-3	PT-3					
PT	PT-03(01)	PT-3(1)	Personally Identifiable Information Processing Purposes | Data Tagging	Personally Identifiable Information Processing Purposes | Data Tagging	PT-3(1)	Not Selected	Functional	Intersects With	5	Data Tagging	PRI-11	Mechanisms exist to issue data modeling guidelines to support tagging of sensitive/regulated data.	PT-3(1)	PT-3(1)	PT-3(1)	PT-3(1)	PT-03(01)	PT-03(01)	PT-03(01)	PT-03(01)	PT-3(1)	PT-3(1)	PT-3(1)	PT-3(1)	PT-3(1)					
PT	PT-03(01)	PT-3(1)	Personally Identifiable Information Processing Purposes | Data Tagging	Personally Identifiable Information Processing Purposes | Data Tagging	PT-3(1)	Not Selected	Functional	Intersects With	5	Data Tags	DCH-22.2	Mechanisms exist to utilize data tags to automate tracking of sensitive/regulated data across the information lifecycle.	PT-3(1)	PT-3(1)	PT-3(1)	PT-3(1)	PT-03(01)	PT-03(01)	PT-03(01)	PT-03(01)	PT-3(1)	PT-3(1)	PT-3(1)	PT-3(1)	PT-3(1)					
PT	PT-03(02)	PT-3(2)	Personally Identifiable Information Processing Purposes | Automation	Personally Identifiable Information Processing Purposes | Automation	PT-3(2)	Not Selected	Functional	Intersects With	5	Automation	PRI-10.1	Automated mechanisms exist to support the evaluation of data quality across the information lifecycle.	PT-3(2)	PT-3(2)	PT-3(2)	PT-3(2)	PT-03(02)	PT-03(02)	PT-03(02)	PT-03(02)	PT-3(2)	PT-3(2)	PT-3(2)	PT-3(2)	PT-3(2)					
PT	PT-03(02)	PT-3(2)	Personally Identifiable Information Processing Purposes | Automation	Personally Identifiable Information Processing Purposes | Automation	PT-3(2)	Not Selected	Functional	Intersects With	5	Automated Data Management Processes	PRI-02.2	Automated mechanisms exist to adjust data that is able to be collected, created, used, disseminated, maintained, retained and/or disclosed, based on updated data subject authorization(s).	PT-3(2)	PT-3(2)	PT-3(2)	PT-3(2)	PT-03(02)	PT-03(02)	PT-03(02)	PT-03(02)	PT-3(2)	PT-3(2)	PT-3(2)	PT-3(2)	PT-3(2)					
PT	PT-04	PT-4	Consent	of their personally identifiable information prior to its	PT-4	Not Selected	Functional	Equal	10	Choice & Consent	PRI-03	(1) Uses plain language and provide examples to illustrate the potential data privacy risks of the authorization; and				PT-4													
PT	PT-04(01)	PT-4(1)	Consent | Tailored Consent	to allow individuals to tailor processing permissions to	PT-4(1)	Not Selected	Functional	Equal	10	Tailored Consent	PRI-03.1	Mechanisms exist to allow data subjects to modify the use permissions to selected attributes of their Personal Data (PD).																		
PT	PT-04(02)	PT-4(2)	Consent | Just-in-time Consent	organization-defined frequency] and in conjunction with	PT-4(2)	Not Selected	Functional	Intersects With	5	Just-In-Time Notice & Updated Consent	PRI-03.2	action, when: (1) The original circumstances under which an individual gave consent have changed; or																		
PT	PT-04(03)	PT-4(3)	Consent | Revocation	mechanisms] for individuals to revoke consent to the	PT-4(3)	Not Selected	Functional	Equal	10	Revoke Consent	PRI-03.4	Mechanisms exist to allow data subjects to revoke consent to the processing of their Personal Data (PD).																		
PT	PT-05	PT-5	Privacy Notice	expressing information about personally identifiable	PT-5	Not Selected	Functional	Intersects With	5	Data Privacy Notice	PRI-02	Personal Data (PD) processing in plain language that meets all legal obligations;				PT-5														
PT	PT-05(01)	PT-5(1)	Privacy Notice | Just-in-time Notice	the individual provides personally identifiable	PT-5(1)	Not Selected	Functional	Intersects With	5	Just-In-Time Notice & Updated Consent	PRI-03.2	action, when: (1) The original circumstances under which an individual gave consent have changed; or																		
PT	PT-05(02)	PT-5(2)	Privacy Notice | Privacy Act Statements	information that will be maintained in a Privacy Act	PT-5(2)	Not Selected	Functional	Equal	10	Privacy Act Statements	PRI-01.2	(2) Whether providing PD is mandatory or optional;				PT-5(2)														
PT	PT-06	PT-6	System of Records Notice	system of records, or provide Privacy Act statements on	PT-6	Not Selected	Functional	Equal	10	System of Records Notice (SORN)	PRI-02.4	Mechanisms exist to draft, publish and keep System of Records Notices (SORN) updated in accordance with regulatory guidance.				PT-6														
PT	PT-06(01)	PT-6(1)	System of Records Notice | Routine Uses	system of records notices to the OMB and appropriate	PT-6(1)	Not Selected	Functional	Equal	10	System of Records Notice (SORN) | Review Process		Mechanisms exist to review all routine uses published in the system of records notice (SORN) to ensure continued accuracy and to ensure that routine uses continue to be compatible with the				PT-6(1)														
PT	PT-06(02)	PT-6(2)	System of Records Notice | Exemption Rules	Records Notice to [Assignment: organization-defined	PT-6(2)	Not Selected	Functional	Equal	10	Privacy Act Exemptions	PRI-02.6	Mechanisms exist to review all Privacy Act exemptions claimed for the System of Records Notices (SORN) to ensure they remain appropriate and accurate.				PT-6(2)														
PT	PT-07	PT-7	Specific Categories of Personally Identifiable Information	frequency] to ensure that they have been	PT-7	Not Selected	Functional	Intersects With	5	Usage Restrictions of Sensitive Personal Data	PRI-05.4	Mechanisms exist to restrict the use of Personal Data (PD) to only the authorized purpose(s) consistent with applicable laws, regulations and in data privacy notices.	PT-7	PT-7	PT-7	PT-7	PT-07	PT-07	PT-07	PT-07	PT-7	PT-7	PT-7	PT-7	PT-7					
PT	PT-07	PT-7	Specific Categories of Personally Identifiable Information	conditions] for specific categories of personally	PT-7	Not Selected	Functional	Intersects With	5	Personal Data Categories	PRI-05.7	Mechanisms exist to define and implement data handling and protection requirements for specific categories of sensitive Personal Data (PD).	PT-7	PT-7	PT-7	PT-7	PT-07	PT-07	PT-07	PT-07	PT-7	PT-7	PT-7	PT-7	PT-7					
PT	PT-07(01)	PT-7(1)	Specific Categories of Personally Identifiable Information | Social Security Numbers	Specific Categories of Personally Identifiable Information | Social Security Numbers	PT-7(1)	Not Selected	Functional	Intersects With	5	Personal Data Categories	PRI-05.7	Mechanisms exist to define and implement data handling and protection requirements for specific categories of sensitive Personal Data (PD).				PT-7(1)														
PT	PT-07(02)	PT-7(2)	Specific Categories of Personally Identifiable Information | First Amendment Information	Specific Categories of Personally Identifiable Information | First Amendment Information	PT-7(2)	Not Selected	Functional	Intersects With	5	Personal Data Categories	PRI-05.7	Mechanisms exist to define and implement data handling and protection requirements for specific categories of sensitive Personal Data (PD).				PT-7(2)														
PT	PT-08	PT-8	Computer Matching Requirements	Federal Register. d. Independently verify the information	PT-8	Not Selected	Functional	Intersects With	5	Computer Matching Agreements (CMA)	PRI-02.3	Mechanisms exist to publish Computer Matching Agreements (CMA) on the public website of the organization.				PT-8														
RA	RA-01	RA-1	Policy and Procedures	implementation of the risk assessment policy and the	RA-1	Low	Functional	Intersects With	5	Cybersecurity & Data Protection	GOV-03	standards and procedures, at planned intervals or if significant changes occur to ensure their	RA-1	RA-1	RA-1	RA-1	RA-01	RA-01	RA-01	RA-01	RA-1	RA-1	RA-1	RA-1	RA-1	RA-01	RA-01	RA-01		RA-01
RA	RA-01	RA-1	Policy and Procedures	implementation of the risk assessment policy and the	RA-1	Low	Functional	Subset Of	10	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	RA-1	RA-1	RA-1	RA-1	RA-01	RA-01	RA-01	RA-01	RA-1	RA-1	RA-1	RA-1	RA-1	RA-01	RA-01	RA-01		RA-01
RA	RA-01	RA-1	Policy and Procedures	implementation of the risk assessment policy and the	RA-1	Low	Functional	Intersects With	5	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	RA-1	RA-1	RA-1	RA-1	RA-01	RA-01	RA-01	RA-01	RA-1	RA-1	RA-1	RA-1	RA-1	RA-01	RA-01	RA-01		RA-01
RA	RA-02	RA-2	Security Categorization	the security plan for the system; and c. Verify that the	RA-2	Low	Functional	Equal	10	Risk-Based Security Categorization	RSK-02	Mechanisms exist to categorize Technology Assets, Applications, Services and/or Data (TASSD) in accordance with applicable laws, regulations and contractual obligations that:	RA-2	RA-2	RA-2		RA-02	RA-02	RA-02	RA-02	RA-2		RA-2	RA-2	RA-2	RA-02	RA-02	RA-02		RA-02
RA	RA-02(01)	RA-2(1)	Security Categorization | Impact-level Prioritization	authorizes, or operates the system or organization-wide	RA-2(1)	Not Selected	Functional	Equal	10	Impact-Level Prioritization	RSK-02.1	Mechanisms exist to prioritize the impact level for Technology Assets, Applications and/or Services (TAAS) to prevent potential disruptions.																		
RA	RA-03	RA-3	Risk Assessment	process perspectives with system-level risk	RA-3	Low	Functional	Intersects With	5	Functional Review Of Cybersecurity & Data Protection Controls	CPL-03.2	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's cybersecurity and data protection policies and standards.	RA-3	RA-3	RA-3	RA-3	RA-03	RA-03	RA-03	RA-03	RA-3	RA-3	RA-3	RA-3	RA-3	RA-03	RA-03	RA-03		RA-03
RA	RA-03	RA-3	Risk Assessment	process perspectives with system-level risk	RA-3	Low	Functional	Intersects With	5	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the	RA-3	RA-3	RA-3	RA-3	RA-03	RA-03	RA-03	RA-03	RA-3	RA-3	RA-3	RA-3	RA-3	RA-03	RA-03	RA-03		RA-03
RA	RA-03(01)	RA-3(1)	Risk Assessment | Supply Chain Risk Assessment	supply chain risk assessment process, results,	RA-3(1)	Low	Functional	Equal	10	Supply Chain Risk Assessment	RSK-09.1	Mechanisms exist to periodically assess supply chain risks associated with Technology Assets, Applications and/or Services (TAAS).	RA-3(1)	RA-3(1)	RA-3(1)		RA-03(01)	RA-03(01)	RA-03(01)	RA-03(01)										
RA	RA-03(02)	RA-3(2)	Risk Assessment | Use of All-source Intelligence	the all-source intelligence to assist in the analysis of	RA-3(2)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
RA	RA-03(03)	RA-3(3)	Risk Assessment | Dynamic Threat Awareness	ongoing basis using [Assignment: organization-defined	RA-3(3)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
RA	RA-03(04)	RA-3(4)	Risk Assessment | Predictive Cyber Analytics	organization-defined systems or system components]	RA-3(4)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
RA	RA-04	RA-4	Withdrawn	Withdrawn	RA-4	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
RA	RA-05	RA-5	Vulnerability Monitoring and Scanning	and procedures; and3. Measuring vulnerability impact.c.	RA-5	Low	Functional	Intersects With	5	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	RA-5	RA-5	RA-5	RA-5	RA-05	RA-05	RA-05	RA-05	RA-5	RA-5	RA-5	RA-5	RA-5	RA-05	RA-05	RA-05	RA-05	RA-05
RA	RA-05	RA-5	Vulnerability Monitoring and Scanning	and procedures; and3. Measuring vulnerability impact.c.	RA-5	Low	Functional	Intersects With	5	Update Tool Capability	VPM-06.1	Mechanisms exist to update vulnerability scanning tools.	RA-5	RA-5	RA-5	RA-5	RA-05	RA-05	RA-05	RA-05	RA-5	RA-5	RA-5	RA-5	RA-5	RA-05	RA-05	RA-05	RA-05	RA-05
RA	RA-05(01)	RA-5(1)	Withdrawn	Withdrawn	RA-5(1)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
RA	RA-05(02)	RA-5(2)	Vulnerability Monitoring and Scanning | Update Vulnerabilities to Be Scanned	Selection (one or more): [Assignment: organization-defined frequency]; prior to a new scan; when new	RA-5(2)	Low	Functional	Intersects With	5	Update Tool Capability	VPM-06.1	Mechanisms exist to update vulnerability scanning tools.	RA-5(2)	RA-5(2)	RA-5(2)		RA-05(02)	RA-05(02)	RA-05(02)	RA-05(02)						RA-05(02)	RA-05(02)	RA-05(02)		RA-05(02)
RA	RA-05(03)	RA-5(3)	Vulnerability Monitoring and Scanning | Breadth and Depth of Coverage	Define the breadth and depth of vulnerability scanning coverage.	RA-5(3)	Not Selected	Functional	Equal	10	Breadth / Depth of Coverage	VPM-06.2	Mechanisms exist to identify the breadth and depth of coverage for vulnerability scanning that define the system components scanned and types of vulnerabilities that are checked for.					RA-05(03)	RA-05(03)	RA-05(03)					RA-5(3)	RA-5(3)			RA-05(03)		RA-05(03)
RA	RA-05(04)	RA-5(4)	Vulnerability Monitoring and Scanning | Discoverable Information	Determine information about the system that is discoverable and take [Assignment: organization-defined	RA-5(4)	High	Functional	Equal	10	Acceptable Discoverable Information	VPM-06.8	Mechanisms exist to define what information is allowed to be discoverable by adversaries and take corrective actions to remediated non-compliant systems.				RA-5(4)				RA-05(04)										RA-05(04)
RA	RA-05(05)	RA-5(5)	Vulnerability Monitoring and Scanning | Privileged Access	[Assignment: organization-defined system components] for [Assignment: organization-defined vulnerability	RA-5(5)	Moderate	Functional	Equal	10	Privileged Access	VPM-06.3	Mechanisms exist to implement privileged access authorization for selected vulnerability scanning activities.		RA-5(5)	RA-5(5)			RA-05(05)	RA-05(05)							RA-05(05)	RA-05(05)		RA-05(05)
RA	RA-05(06)	RA-5(6)	Vulnerability Monitoring and Scanning | Automated Trend Analyses	[Assignment: organization-defined automated	RA-5(6)	Not Selected	Functional	Equal	10	Trend Analysis	VPM-06.4	Automated mechanisms exist to compare the results of vulnerability scans over time to determine trends in system vulnerabilities.												RA-5(6)	RA-5(6)				RA-05(06)		RA-05(06)
RA	RA-05(07)	RA-5(7)	Withdrawn	Withdrawn	RA-5(7)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
RA	RA-05(08)	RA-5(8)	Vulnerability Monitoring and Scanning | Review Historic Audit Logs	identified in a [Assignment: organization-defined system] has been previously exploited within an	RA-5(8)	Not Selected	Functional	Equal	10	Review Historical event logs	VPM-06.5	Mechanisms exist to review historical event logs to determine if identified vulnerabilities have been previously exploited.							RA-05(08)										RA-05(08)		RA-05(08)
RA	RA-05(09)	RA-5(9)	Withdrawn	Withdrawn	RA-5(9)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
RA	RA-05(10)	RA-5(10)	Vulnerability Monitoring and Scanning | Correlate Scanning Information	determine the presence of multi-vulnerability and multi-	RA-5(10)	Not Selected	Functional	Equal	10	Correlate Scanning Information	VPM-06.9	Automated mechanisms exist to correlate the output from vulnerability scanning tools to determine the presence of multi-vulnerability/multi-hop attack vectors.																		RA-05(10)
RA	RA-05(11)	RA-5(11)	Vulnerability Monitoring and Scanning | Public Disclosure Program	of vulnerabilities in organizational systems and system	RA-5(11)	Low	Functional	Equal	10	Vulnerability Disclosure Program (VDP)	THR-06	Mechanisms exist to establish a Vulnerability Disclosure Program (VDP) to assist with the secure development and maintenance of Technology Assets, Applications and/or Services (TAAS) that receives	RA-5(11)	RA-5(11)	RA-5(11)		RA-05(11)	RA-05(11)	RA-05(11)	RA-05(11)										
RA	RA-06	RA-6	Technical Surveillance Countermeasures Survey	Selection (one or more): [Assignment: organization-defined frequency]; when the following events or	RA-6	Not Selected	Functional	Equal	10	Technical Surveillance Countermeasures Security	VPM-08	Mechanisms exist to utilize a technical surveillance countermeasures survey.																		
RA	RA-07	RA-7	Risk Response	assessments, monitoring, and audits in accordance with	RA-7	Low	Functional	Equal	10	Risk Response	RSK-06.1	Mechanisms exist to respond to findings from cybersecurity and data protection assessments, incidents and audits to ensure proper remediation has been performed.	RA-7	RA-7	RA-7	RA-7	RA-07	RA-07	RA-07	RA-07	RA-7		RA-7	RA-7	RA-7					
RA	RA-08	RA-8	Privacy Impact Assessments	and2. Includes personally identifiable information	RA-8	Not Selected	Functional	Equal	10	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify				RA-8														
RA	RA-09	RA-9	Criticality Analysis	organization-defined systems, system components, or	RA-9	Moderate	Functional	Intersects With	5	Third-Party Criticality Assessments	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their	RA-9	RA-9	RA-9	RA-9	RA-09	RA-09	RA-09	RA-09	RA-9	RA-9	RA-9	RA-9	RA-9					
RA	RA-09	RA-9	Criticality Analysis	organization-defined systems, system components, or	RA-9	Moderate	Functional	Intersects With	5	Criticality Analysis	TDA-06.1	Mechanisms exist to require the developer of the Technology Asset, Application and/or Service (TAAS) to perform a criticality analysis at organization-defined decision points in the Secure Development Life	RA-9	RA-9	RA-9	RA-9	RA-09	RA-09	RA-09	RA-09	RA-9	RA-9	RA-9	RA-9	RA-9					
RA	RA-09	RA-9	Criticality Analysis	organization-defined systems, system components, or	RA-9	Moderate	Functional	Intersects With	5	Cybersecurity & Data Protection Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical Technology Assets, Applications and/or Services (TAAS) at pre-defined decision	RA-9	RA-9	RA-9	RA-9	RA-09	RA-09	RA-09	RA-09	RA-9	RA-9	RA-9	RA-9	RA-9					
RA	RA-10	RA-10	Threat Hunting	organization-defined systems and2. Detect, track, and disrupt	RA-10	Not Selected	Functional	Equal	10	Threat Hunting	THR-07	Mechanisms exist to perform cyber threat hunting that uses Indicators of Compromise (IoC) to detect, track and disrupt threats that evade existing security controls.													RA-10	RA-10				
SA	SA-01	SA-1	Policy and Procedures	acquisition policy and the associated system and	SA-1	Low	Functional	Intersects With	5	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	SA-1	SA-1	SA-1	SA-1	SA-01	SA-01	SA-01	SA-01	SA-1	SA-1	SA-1	SA-1	SA-1	SA-01	SA-01	SA-01		SA-01
SA	SA-01	SA-1	Policy and Procedures	acquisition policy and the associated system and	SA-1	Low	Functional	Subset Of	10	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	SA-1	SA-1	SA-1	SA-1	SA-01	SA-01	SA-01	SA-01	SA-1	SA-1	SA-1	SA-1	SA-1	SA-01	SA-01	SA-01		SA-01
SA	SA-01	SA-1	Policy and Procedures	acquisition policy and the associated system and	SA-1	Low	Functional	Intersects With	5	Cybersecurity & Data Protection Governance Program	GOV-03	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures, at planned intervals or if significant changes occur to ensure their	SA-1	SA-1	SA-1	SA-1	SA-01	SA-01	SA-01	SA-01	SA-1	SA-1	SA-1	SA-1	SA-1	SA-01	SA-01	SA-01		SA-01
SA	SA-01	SA-1	Policy and Procedures	acquisition policy and the associated system and	SA-1	Low	Functional	Intersects With	5	Secure Coding	TDA-06	Mechanisms exist to develop applications based on secure coding principles.	SA-1	SA-1	SA-1	SA-1	SA-01	SA-01	SA-01	SA-01	SA-1	SA-1	SA-1	SA-1	SA-1	SA-01	SA-01	SA-01		SA-01
SA	SA-02	SA-2	Allocation of Resources	protect the system or system service as part of the	SA-2	Low	Functional	Equal	10	Allocation of Resources	PRM-03	Mechanisms exist to identify and allocate resources for management, operational, technical and data protection requirements within business process planning for projects / initiatives.	SA-2	SA-2	SA-2	SA-2	SA-02	SA-02	SA-02	SA-02	SA-2		SA-2	SA-2	SA-2	SA-02	SA-02	SA-02		SA-02
SA	SA-03	SA-3	System Development Life Cycle	responsibilities throughout the system development life	SA-3	Low	Functional	Intersects With	5	Technology Lifecycle Management	SEA-07.1	Mechanisms exist to manage the usable lifecycles of Technology Assets, Applications and/or Services (TAAS).	SA-3	SA-3	SA-3	SA-3	SA-03	SA-03	SA-03	SA-03	SA-3	SA-3	SA-3	SA-3	SA-3	SA-03	SA-03	SA-03		SA-03
SA	SA-03	SA-3	System Development Life Cycle	responsibilities throughout the system development life	SA-3	Low	Functional	Intersects With	5	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	SA-3	SA-3	SA-3	SA-3	SA-03	SA-03	SA-03	SA-03	SA-3	SA-3	SA-3	SA-3	SA-3	SA-03	SA-03	SA-03		SA-03
SA	SA-03(01)	SA-3(1)	System Development Life Cycle | Manage Preproduction Environment	commensurate with risk throughout the system	SA-3(1)	Not Selected	Functional	Intersects With	5	Technology Lifecycle Management	SEA-07.1	Mechanisms exist to manage the usable lifecycles of Technology Assets, Applications and/or Services (TAAS).	SA-3(1)	SA-3(1)	SA-3(1)	SA-3(1)	SA-03(01)	SA-03(01)	SA-03(01)	SA-03(01)	SA-3(1)	SA-3(1)	SA-3(1)	SA-3(1)	SA-3(1)					
SA	SA-03(01)	SA-3(1)	System Development Life Cycle | Manage Preproduction Environment	commensurate with risk throughout the system	SA-3(1)	Not Selected	Functional	Intersects With	5	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	SA-3(1)	SA-3(1)	SA-3(1)	SA-3(1)	SA-03(01)	SA-03(01)	SA-03(01)	SA-03(01)	SA-3(1)	SA-3(1)	SA-3(1)	SA-3(1)	SA-3(1)					
SA	SA-03(01)	SA-3(1)	System Development Life Cycle | Manage Preproduction Environment	commensurate with risk throughout the system	SA-3(1)	Not Selected	Functional	Intersects With	5	Secure Development Environments	TDA-07	Mechanisms exist to maintain a segmented development network to ensure a secure development environment.	SA-3(1)	SA-3(1)	SA-3(1)	SA-3(1)	SA-03(01)	SA-03(01)	SA-03(01)	SA-03(01)	SA-3(1)	SA-3(1)	SA-3(1)	SA-3(1)	SA-3(1)					
SA	SA-03(02)	SA-3(2)	System Development Life Cycle | Use of Live or Operational Data	preproduction environments for the system, system	SA-3(2)	Not Selected	Functional	Equal	10	Use of Live Data	TDA-10	Mechanisms exist to approve, document and control the use of live data in development and test environments.																		
SA	SA-03(03)	SA-3(3)	System Development Life Cycle | Technology Refresh	for the system throughout the system development life	SA-3(3)	Not Selected	Functional	Intersects With	5	Technology Lifecycle Management	SEA-07.1	Mechanisms exist to manage the usable lifecycles of Technology Assets, Applications and/or Services (TAAS).	SA-3(3)	SA-3(3)	SA-3(3)	SA-3(3)	SA-03(03)	SA-03(03)	SA-03(03)	SA-03(03)	SA-3(3)	SA-3(3)	SA-3(3)	SA-3(3)	SA-3(3)					
SA	SA-03(03)	SA-3(3)	System Development Life Cycle | Technology Refresh	for the system throughout the system development life	SA-3(3)	Not Selected	Functional	Intersects With	5	Refresh from Trusted Sources	SEA-08.1	Mechanisms exist to ensure that software and data needed for system component and service outages are obtained from trusted sources.	SA-3(3)	SA-3(3)	SA-3(3)	SA-3(3)	SA-03(03)	SA-03(03)	SA-03(03)	SA-03(03)	SA-3(3)	SA-3(3)	SA-3(3)	SA-3(3)	SA-3(3)					
SA	SA-04	SA-4	Acquisition Process	needed to satisfy the security and privacy	SA-4	Low	Functional	Intersects With	5	Minimum Viable Product (MVP) Security Requirements	TDA-02	Mechanisms exist to design, develop and produce Technology Assets, Applications and/or Services (TAAS) in such a way that risk-based technical and functional specifications ensure Minimum Viable	SA-4	SA-4	SA-4	SA-4	SA-04	SA-04	SA-04	SA-04	SA-4	SA-4	SA-4	SA-4	SA-4		SA-04		SA-04	SA-04
SA	SA-04	SA-4	Acquisition Process	needed to satisfy the security and privacy	SA-4	Low	Functional	Intersects With	5	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	SA-4	SA-4	SA-4	SA-4	SA-04	SA-04	SA-04	SA-04	SA-4	SA-4	SA-4	SA-4	SA-4		SA-04		SA-04	SA-04
SA	SA-04	SA-4	Acquisition Process	needed to satisfy the security and privacy	SA-4	Low	Functional	Intersects With	5	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	SA-4	SA-4	SA-4	SA-4	SA-04	SA-04	SA-04	SA-04	SA-4	SA-4	SA-4	SA-4	SA-4		SA-04		SA-04	SA-04
SA	SA-04	SA-4	Acquisition Process	needed to satisfy the security and privacy	SA-4	Low	Functional	Intersects With	5	Managing Changes To Third-Party Services	TPM-10	M

Family	Sorting Control #	Focal Document Element	Focal Document Element Name	Focal Document Element Description	NIST SP 800-53 R5.2	Security Control Baseline	Set Theory Relationship Mapping (STRM) Rationale	Relationship	Strength of Relationship	Reference Document Element	Reference Document Name	Reference Document Element Description	NIST SP 800-53 R5.2 Baselines Low	Mod	High	Privacy	FedRAMP R5 Low	Mod	High	LI-SaaS	C-SCRM Baseline	NIST SP 800-161 R1 Low Impact Level Down Overlay	Level 1	Level 2	Level 3	GovRAMP Low	Low+	Moderate	Core	High (FedRAMP Int.)
SA	SA-05	SA-5	System Documentation	effectively use those functions and mechanisms;2.	SA-5	Low	Functional	Intersects With	5	Asset Scope Classification	AST-04.1	Mechanisms exist to determine cybersecurity and data protection control applicability by identifying, assigning and documenting the appropriate asset scope categorization for all Technology Assets.	SA-5	SA-5	SA-5	SA-5	SA-05	SA-05	SA-05	SA-05	SA-5	SA-5	SA-5	SA-5	SA-5	SA-05	SA-05	SA-05		SA-05
SA	SA-05(01)	SA-5(1)		Withdrawn	SA-5(1)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
SA	SA-05(02)	SA-5(2)		Withdrawn	SA-5(2)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
SA	SA-05(03)	SA-5(3)		Withdrawn	SA-5(3)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
SA	SA-05(04)	SA-5(4)		Withdrawn	SA-5(4)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
SA	SA-05(05)	SA-5(5)		Withdrawn	SA-5(5)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
SA	SA-06	SA-6		Withdrawn	SA-6	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
SA	SA-07	SA-7		Withdrawn	SA-7	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
SA	SA-08	SA-8	Security and Privacy Engineering Principles	development, implementation, and modification of the	SA-8	Low	Functional	Intersects With	5	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system	SA-8	SA-8	SA-8	SA-8	SA-08	SA-08	SA-08	SA-08	SA-8	SA-8	SA-8	SA-8	SA-8			SA-08		SA-08
SA	SA-08	SA-8	Security and Privacy Engineering Principles	development, implementation, and modification of the	SA-8	Low	Functional	Intersects With	5	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity and data protection practices in the specification, design, development, implementation and modification of	SA-8	SA-8	SA-8	SA-8	SA-08	SA-08	SA-08	SA-08	SA-8	SA-8	SA-8	SA-8	SA-8			SA-08		SA-08
SA	SA-08(01)	SA-8(1)	Security and Privacy Engineering Principles | Clear Abstractions	Implement the security design principle of clear	SA-8(1)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SA	SA-08(02)	SA-8(2)	Security and Privacy Engineering Principles | Least Common Mechanism	mechanism in [Assignment: organization-defined	SA-8(2)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SA	SA-08(03)	SA-8(3)	Security and Privacy Engineering Principles | Modularity and Layering	and layering in [Assignment: organization-defined	SA-8(3)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SA	SA-08(04)	SA-8(4)	Security and Privacy Engineering Principles | Partially Ordered Dependencies	ordered dependencies in [Assignment: organization-	SA-8(4)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SA	SA-08(05)	SA-8(5)	Security and Privacy Engineering Principles | Efficiently Mediated Access	mediated access in [Assignment: organization-defined	SA-8(5)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SA	SA-08(06)	SA-8(6)	Security and Privacy Engineering Principles | Minimized Sharing	sharing in [Assignment: organization-defined systems or	SA-8(6)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SA	SA-08(07)	SA-8(7)	Security and Privacy Engineering Principles | Reduced Complexity	complexity in [Assignment: organization-defined	SA-8(7)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SA	SA-08(08)	SA-8(8)	Security and Privacy Engineering Principles | Secure Evolvability	evolvability in [Assignment: organization-defined	SA-8(8)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SA	SA-08(09)	SA-8(9)	Security and Privacy Engineering Principles | Trusted Components	components in [Assignment: organization-defined	SA-8(9)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SA	SA-08(10)	SA-8(10)	Security and Privacy Engineering Principles | Hierarchical Trust	trust in [Assignment: organization-defined systems or	SA-8(10)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SA	SA-08(11)	SA-8(11)	Security and Privacy Engineering Principles | Inverse Modification Threshold	modification threshold in [Assignment: organization-	SA-8(11)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SA	SA-08(12)	SA-8(12)	Security and Privacy Engineering Principles | Hierarchical Protection	protection in [Assignment: organization-defined systems	SA-8(12)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SA	SA-08(13)	SA-8(13)	Security and Privacy Engineering Principles | Minimized Security Elements	security elements in [Assignment: organization-defined	SA-8(13)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SA	SA-08(14)	SA-8(14)	Security and Privacy Engineering Principles | Least Privilege	in [Assignment: organization-defined systems or system	SA-8(14)	Not Selected	Functional	Equal	10	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.																		
SA	SA-08(15)	SA-8(15)	Security and Privacy Engineering Principles | Predicate Permission	permission in [Assignment: organization-defined	SA-8(15)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SA	SA-08(16)	SA-8(16)	Security and Privacy Engineering Principles | Self-reliant Trustworthiness	trustworthiness in [Assignment: organization-defined	SA-8(16)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SA	SA-08(17)	SA-8(17)	Security and Privacy Engineering Principles | Secure Distributed Composition	distributed composition in [Assignment: organization-	SA-8(17)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SA	SA-08(18)	SA-8(18)	Security and Privacy Engineering Principles | Trusted Communications Channels	communications channels in [Assignment: organization-	SA-8(18)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SA	SA-08(19)	SA-8(19)	Security and Privacy Engineering Principles | Continuous Protection	protection in [Assignment: organization-defined systems	SA-8(19)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SA	SA-08(20)	SA-8(20)	Security and Privacy Engineering Principles | Secure Metadata Management	metadata management in [Assignment: organization-	SA-8(20)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SA	SA-08(21)	SA-8(21)	Security and Privacy Engineering Principles | Self-Analysis	in [Assignment: organization-defined systems or system	SA-8(21)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SA	SA-08(22)	SA-8(22)	Security and Privacy Engineering Principles | Accountability and Traceability	and traceability in [Assignment: organization-defined	SA-8(22)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SA	SA-08(23)	SA-8(23)	Security and Privacy Engineering Principles | Secure Defaults	defaults in [Assignment: organization-defined systems or	SA-8(23)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SA	SA-08(24)	SA-8(24)	Security and Privacy Engineering Principles | Secure Failure and Recovery	and recovery in [Assignment: organization-defined	SA-8(24)	Not Selected	Functional	Equal	10	Fail Secure	SEA-07.2	Mechanisms exist to enable systems to fail to an organization-defined known-state for types of failures, preserving system state information in failure.																		
SA	SA-08(25)	SA-8(25)	Security and Privacy Engineering Principles | Economic Security	security in [Assignment: organization-defined systems or	SA-8(25)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SA	SA-08(26)	SA-8(26)	Security and Privacy Engineering Principles | Performance Security	security in [Assignment: organization-defined systems or	SA-8(26)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SA	SA-08(27)	SA-8(27)	Security and Privacy Engineering Principles | Human Factored Security	factored security in [Assignment: organization-defined	SA-8(27)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SA	SA-08(28)	SA-8(28)	Security and Privacy Engineering Principles | Acceptable Security	security in [Assignment: organization-defined systems or	SA-8(28)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SA	SA-08(29)	SA-8(29)	Security and Privacy Engineering Principles | Repeatable and Documented Procedures	and documented procedures in [Assignment:	SA-8(29)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SA	SA-08(30)	SA-8(30)	Security and Privacy Engineering Principles | Procedural Rigor	rigor in [Assignment: organization-defined systems or	SA-8(30)	Not Selected	Functional	Intersects With	5	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	SA-8(30)	SA-8(30)	SA-8(30)	SA-8(30)	SA-08(30)	SA-08(30)	SA-08(30)	SA-08(30)	SA-8(30)	SA-8(30)	SA-8(30)	SA-8(30)	SA-8(30)					
SA	SA-08(30)	SA-8(30)	Security and Privacy Engineering Principles | Procedural Rigor	rigor in [Assignment: organization-defined systems or	SA-8(30)	Not Selected	Functional	Intersects With	5	Technology Lifecycle Management	SEA-07.1	Mechanisms exist to manage the usable lifecycles of Technology Assets, Applications and/or Services (TAAS).	SA-8(30)	SA-8(30)	SA-8(30)	SA-8(30)	SA-08(30)	SA-08(30)	SA-08(30)	SA-08(30)	SA-8(30)	SA-8(30)	SA-8(30)	SA-8(30)	SA-8(30)					
SA	SA-08(31)	SA-8(31)	Security and Privacy Engineering Principles | Secure System Modification	system modification in [Assignment: organization-	SA-8(31)	Not Selected	Functional	Intersects With	5	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	SA-8(31)	SA-8(31)	SA-8(31)	SA-8(31)	SA-08(31)	SA-08(31)	SA-08(31)	SA-08(31)	SA-8(31)	SA-8(31)	SA-8(31)	SA-8(31)	SA-8(31)					
SA	SA-08(31)	SA-8(31)	Security and Privacy Engineering Principles | Secure System Modification	modification in [Assignment: organization-	SA-8(31)	Not Selected	Functional	Intersects With	5	Control Functionality Verification	CHG-06	Mechanisms exist to verify the functionality of cybersecurity and/or data privacy controls following implemented changes to ensure applicable controls operate as designed.	SA-8(31)	SA-8(31)	SA-8(31)	SA-8(31)	SA-08(31)	SA-08(31)	SA-08(31)	SA-08(31)	SA-8(31)	SA-8(31)	SA-8(31)	SA-8(31)	SA-8(31)					
SA	SA-08(31)	SA-8(31)	Security and Privacy Engineering Principles | Secure System Modification	system modification in [Assignment: organization-	SA-8(31)	Not Selected	Functional	Intersects With	5	Test, Validate & Document Changes	CHG-02.2	Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented in a production environment.	SA-8(31)	SA-8(31)	SA-8(31)	SA-8(31)	SA-08(31)	SA-08(31)	SA-08(31)	SA-08(31)	SA-8(31)	SA-8(31)	SA-8(31)	SA-8(31)	SA-8(31)					
SA	SA-08(32)	SA-8(32)	Security and Privacy Engineering Principles | Sufficient Documentation	documentation in [Assignment: organization-defined	SA-8(32)	Not Selected	Functional	Equal	10	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.																		
SA	SA-08(33)	SA-8(33)	Security and Privacy Engineering Principles | Minimization	Implement the privacy principle of minimization using	SA-8(33)	Not Selected	Functional	Intersects With	5	Collection Minimization	END-13.3	Mechanisms exist to utilize sensors that are configured to minimize the collection of information about individuals.	SA-8(33)	SA-8(33)	SA-8(33)	SA-8(33)	SA-08(33)	SA-08(33)	SA-08(33)	SA-08(33)	SA-8(33)	SA-8(33)	SA-8(33)	SA-8(33)	SA-8(33)					
SA	SA-08(33)	SA-8(33)	Security and Privacy Engineering Principles | Minimization	Implement the privacy principle of minimization using	SA-8(33)	Not Selected	Functional	Intersects With	5	Limit Sensitive / Regulated Data In Testing, Training & Research	DCH-18.2	Mechanisms exist to minimize the use of sensitive/regulated data for research, testing, or training, in accordance with authorized, legitimate business practices.	SA-8(33)	SA-8(33)	SA-8(33)	SA-8(33)	SA-08(33)	SA-08(33)	SA-08(33)	SA-08(33)	SA-8(33)	SA-8(33)	SA-8(33)	SA-8(33)	SA-8(33)					
SA	SA-08(33)	SA-8(33)	Security and Privacy Engineering Principles | Minimization	Implement the privacy principle of minimization using	SA-8(33)	Not Selected	Functional	Intersects With	5	Minimize Visitor Personal Data (PD)	PES-06.5	Mechanisms exist to minimize the collection of Personal Data (PD) contained in visitor access records.	SA-8(33)	SA-8(33)	SA-8(33)	SA-8(33)	SA-08(33)	SA-08(33)	SA-08(33)	SA-08(33)	SA-8(33)	SA-8(33)	SA-8(33)	SA-8(33)	SA-8(33)					
SA	SA-09	SA-9	External System Services	and responsibilities with regard to external system	SA-9	Low	Functional	Equal	10	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	SA-9	SA-9	SA-9	SA-9	SA-09	SA-09	SA-09	SA-09						SA-09	SA-09	SA-09		SA-09
SA	SA-09(01)	SA-9(1)	External System Services | Risk Assessments and Organizational Approvals	services; and\b. Verify that the acquisition or outsourcing of dedicated information security services is approved	SA-9(1)	Not Selected	Functional	Equal	10	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).					SA-09(01)	SA-09(01)				SA-9(1)	SA-9(1)			SA-09(01)	SA-09(01)			SA-09(01)
SA	SA-09(02)	SA-9(2)	External System Services | Identification of Functions, Ports, Protocols, and Services	other services required for the use of such services:	SA-9(2)	Moderate	Functional	Equal	10	Identification of Ports, Protocols & Services	TPM-04.2	Mechanisms exist to require External Service Providers (ESPs) to identify and document the business need for ports, protocols and other services it requires to operate its Technology Assets, Applications		SA-9(2)	SA-9(2)			SA-09(02)	SA-09(02)							SA-09(02)	SA-09(02)		SA-09(02)
SA	SA-09(03)	SA-9(3)	External System Services | Establish and Maintain Trust Relationship with Providers	requirements, properties, factors, or conditions	SA-9(3)	Not Selected	Functional	Intersects With	5	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those												SA-9(3)	SA-9(3)	SA-9(3)					
SA	SA-09(03)	SA-9(3)	External System Services | Establish and Maintain Trust Relationship with Providers	requirements, properties, factors, or conditions	SA-9(3)	Not Selected	Functional	Intersects With	5	Conflict of Interests	TPM-04.3	Mechanisms exist to ensure that the interests of external service providers are consistent with and reflect organizational interests.												SA-9(3)	SA-9(3)	SA-9(3)					
SA	SA-09(03)	SA-9(3)	External System Services | Establish and Maintain Trust Relationship with Providers	requirements, properties, factors, or conditions	SA-9(3)	Not Selected	Functional	Intersects With	5	Third-Party Criticality Assessments	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their												SA-9(3)	SA-9(3)	SA-9(3)					
SA	SA-09(03)	SA-9(3)	External System Services | Establish and Maintain Trust Relationship with Providers	requirements, properties, factors, or conditions	SA-9(3)	Not Selected	Functional	Intersects With	5	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to implement a Supply Chain Risk Management (SCRM) strategy and associated processes to identify, assess, mitigate and monitor the supply chain risks across the Technology Assets, Applications and/or Services (TAAS) supply chains; and												SA-9(3)	SA-9(3)	SA-9(3)					
SA	SA-09(03)	SA-9(3)	External System Services | Establish and Maintain Trust Relationship with Providers	requirements, properties, factors, or conditions	SA-9(3)	Not Selected	Functional	Intersects With	5	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans, as well as in the event a plan must be activated to respond to events. Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity and data												SA-9(3)	SA-9(3)	SA-9(3)					
SA	SA-09(03)	SA-9(3)	External System Services | Establish and Maintain Trust Relationship with Providers	requirements, properties, factors, or conditions	SA-9(3)	Not Selected	Functional	Intersects With	5	Break Clauses	TPM-05.7	Mechanisms exist to include "break clauses" within contracts for failure to meet contract criteria for cybersecurity and/or data protection controls.												SA-9(3)	SA-9(3)	SA-9(3)					
SA	SA-09(04)	SA-9(4)	External System Services | Consistent Interests of Consumers and Providers	Take the following actions to verify that the interests of external service providers are consistent with and	SA-9(4)	Not Selected	Functional	Equal	10	Conflict of Interests	TPM-04.3	Mechanisms exist to ensure that the interests of external service providers are consistent with and reflect organizational interests.												SA-9(4)							SA-09(04)
SA	SA-09(05)	SA-9(5)	External System Services | Processing, Storage, and Service Location	services] to [Assignment: organization-defined locations]	SA-9(5)	Not Selected	Functional	Intersects With	5	Processing, Storage and Service Location	CLD-09	Mechanisms exist to restrict the location of cloud processing/storage based on business requirements that includes statutory, regulatory and contractual obligations.	SA-9(5)	SA-9(5)	SA-9(5)	SA-9(5)	SA-09(05)	SA-09(05)	SA-09(05)	SA-09(05)	SA-9(5)	SA-9(5)	SA-9(5)	SA-9(5)	SA-9(5)					SA-09(05)
SA	SA-09(05)	SA-9(5)	External System Services | Processing, Storage, and Service Location	services] to [Assignment: organization-defined locations]	SA-9(5)	Not Selected	Functional	Intersects With	5	Third-Party Processing, Storage and Service Location	TPM-04.4	Mechanisms exist to restrict the location of information processing/storage based on business requirements.	SA-9(5)	SA-9(5)	SA-9(5)	SA-9(5)	SA-09(05)	SA-09(05)	SA-09(05)	SA-09(05)	SA-9(5)	SA-9(5)	SA-9(5)	SA-9(5)	SA-9(5)					SA-09(05)
SA	SA-09(05)	SA-9(5)	External System Services | Processing, Storage, and Service Location	services] to [Assignment: organization-defined locations]	SA-9(5)	Not Selected	Functional	Intersects With	5	Geographic Location of Data	DCH-19	Mechanisms exist to inventory, document and maintain data flows for data that is resident (permanently or temporarily) within the service's geographically distributed applications (physical and	SA-9(5)	SA-9(5)	SA-9(5)	SA-9(5)	SA-09(05)	SA-09(05)	SA-09(05)	SA-09(05)	SA-9(5)	SA-9(5)	SA-9(5)	SA-9(5)	SA-9(5)					SA-09(05)
SA	SA-09(06)	SA-9(6)	External System Services | Organization-controlled Cryptographic Keys	encrypted material stored or transmitted through an	SA-9(6)	Not Selected	Functional	Equal	10	External System Cryptographic Key Control	CRY-09.7	Mechanisms exist to maintain control of cryptographic keys for encrypted material stored or transmitted through an external system.																		
SA	SA-09(07)	SA-9(7)	External System Services | Organization-controlled Integrity Checking	Provide the capability to check the integrity of	SA-9(7)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SA	SA-09(08)	SA-9(8)	External System Services | Processing and Storage Location — U.S. Jurisdiction	processing and data storage to facilities located within in	SA-9(8)	Not Selected	Functional	Intersects With	5	Geographic Location of Data	DCH-19	Mechanisms exist to inventory, document and maintain data flows for data that is resident (permanently or temporarily) within a service's geographically distributed applications (physical and	SA-9(8)	SA-9(8)	SA-9(8)	SA-9(8)	SA-09(08)	SA-09(08)	SA-09(08)	SA-09(08)	SA-9(8)	SA-9(8)	SA-9(8)	SA-9(8)	SA-9(8)					
SA	SA-09(08)	SA-9(8)	External System Services | Processing and Storage Location — U.S. Jurisdiction	processing and data storage to facilities located within in	SA-9(8)	Not Selected	Functional	Intersects With	5	Processing, Storage and Service Location	CLD-09	Mechanisms exist to restrict the location of cloud processing/storage based on business requirements that includes statutory, regulatory and contractual obligations.	SA-9(8)	SA-9(8)	SA-9(8)	SA-9(8)	SA-09(08)	SA-09(08)	SA-09(08)	SA-09(08)	SA-9(8)	SA-9(8)	SA-9(8)	SA-9(8)	SA-9(8)					
SA	SA-10	SA-10	Developer Configuration Management	under configuration management\c. Implement only	SA-10	Moderate	Functional	Equal	10	Developer Configuration Management	TDA-14	Mechanisms exist to require system developers and integrators to perform configuration management during system design, development, implementation and operation.		SA-10	SA-10			SA-10	SA-10				SA-10	SA-10			SA-10		SA-10	
SA	SA-10(01)	SA-10(1)	Developer Configuration Management | Software and Firmware Integrity Verification	component, or system service to enable integrity	SA-10(1)	Not Selected	Functional	Equal	10	Software / Firmware Integrity Verification	TDA-14.1	Mechanisms exist to require developers of Technology Assets, Applications and/or Services (TAAS) to enable integrity verification of software and firmware components.																SA-10(01)			SA-10(01)
SA	SA-10(02)	SA-10(2)	Developer Configuration Management | Alternative Configuration Management Processes	using organizational personnel in the absence of a	SA-10(2)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SA	SA-10(03)	SA-10(3)	Developer Configuration Management | Hardware Integrity Verification	component, or system service to enable integrity	SA-10(3)	Not Selected	Functional	Equal	10	Hardware Integrity Verification	TDA-14.2	Mechanisms exist to require developers of Technology Assets, Applications and/or Services (TAAS) to enable integrity verification of hardware components.																		
SA	SA-10(04)	SA-10(4)	Developer Configuration Management | Trusted Generation	comparing newly generated versions of security-relevant	SA-10(4)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SA	SA-10(05)	SA-10(5)	Developer Configuration Management | Mapping Integrity for Version Control	of the mapping between the master build data	SA-10(5)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SA	SA-10(06)	SA-10(6)	Developer Configuration Management | Trusted Distribution	ensuring that security-relevant hardware, software, and	SA-10(6)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SA	SA-10(07)	SA-10(7)	Developer Configuration Management | Security and Privacy Representatives	privacy representatives] to be included in the	SA-10(7)	Not Selected	Functional	Equal	10	Cybersecurity & Data Protection Representatives For Product Changes	TDA-02.7	Mechanisms exist to include appropriate cybersecurity and data protection representatives in the product feature and/or functionality change control review process.																		
SA	SA-11	SA-11	Developer Testing and Evaluation	[Assignment: organization-defined frequency] at	SA-11	Moderate	Functional	Equal	10	Cybersecurity & Data Protection Testing Throughout Development	TDA-09	(1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified		SA-11	SA-11	SA-11		SA-11	SA-11				SA-11	SA-11	SA-11		SA-11	SA-11	SA-11	SA-11
SA	SA-11(01)	SA-11(1)	Developer Testing and Evaluation | Static Code Analysis	component, or system service to employ static code	SA-11(1)	Not Selected	Functional	Equal	10	Static Code Analysis	TDA-09.2	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to employ static code analysis tools to identify and remediate common flaws and document the results						SA-11(01)	SA-11(01)									SA-11(01)	SA-11(01)	SA-11(01)
SA	SA-11(02)	SA-11(2)	Developer Testing and Evaluation | Threat Modeling and Vulnerability Analyses	operations, known or assumed threats, and acceptable	SA-11(2)	Not Selected	Functional	Intersects With	5	Developer Threat Analysis & Flaw Remediation	TDA-15	Mechanisms exist to require the developer of the system, system component or service to create and implement a Security Testing and Evaluation (ST&E) plan, or similar process, to objectively identify and remediate	SA-11(2)	SA-11(2)	SA-11(2)	SA-11(2)	SA-11(02)	SA-11(02)	SA-11(02)	SA-11(02)	SA-11(2)	SA-11(2)	SA-11(2)	SA-11(2)	SA-11(2)			SA-11(02)		SA-11(02)
SA	SA-11(02)	SA-11(2)	Developer Testing and Evaluation | Threat Modeling and Vulnerability Analyses	operations, known or assumed threats, and acceptable	SA-11(2)	Not Selected	Functional	Intersects With	5	Threat Modeling	TDA-06.2	Mechanisms exist to perform threat modeling and other secure design techniques, to ensure that threats to software and solutions are identified and accounted for.	SA-11(2)	SA-11(2)	SA-11(2)	SA-11(2)	SA-11(02)	SA-11(02)	SA-11(02)	SA-11(02)	SA-11(2)	SA-11(2)	SA-11(2)	SA-11(2)	SA-11(2)			SA-11(02)		SA-11(02)
SA	SA-11(03)	SA-11(3)	Developer Testing and Evaluation | Independent Verification of Assessment Plans and Evidence	privacy assessment plans and the evidence produced	SA-11(3)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SA	SA-11(04)	SA-11(4)	Developer Testing and Evaluation | Manual Code Review	review of [Assignment: organization-defined specific	SA-11(4)	Not Selected	Functional	Equal	10	Manual Code Review	TDA-09.7	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to employ a manual code review process to identify and remediate unique flaws that require knowledge																		
SA	SA-11(05)	SA-11(5)	Developer Testing and Evaluation | Penetration Testing	testing: a. At the following level of rigor: [Assignment:	SA-11(5)	Not Selected	Functional	Intersects With	5	Threat Analysis & Flaw Remediation During Development	IAO-04	Mechanisms exist to require system developers/integrators to create and implement a Security Testing and Evaluation (ST&E) plan, or similar process, to identify and remediate flaws during	SA-11(5)	SA-11(5)	SA-11(5)	SA-11(5)	SA-11(05)	SA-11(05)	SA-11(05)	SA-11(05)	SA-11(5)	SA-11(5)	SA-11(5)	SA-11(5)	SA-11(5)					
SA	SA-11(05)	SA-11(5)	Developer Testing and Evaluation | Penetration Testing	testing: a. At the following level of rigor: [Assignment:	SA-11(5)	Not Selected	Functional	Intersects With	5	Application Penetration Testing	TDA-09.5	Mechanisms exist to perform application-level penetration testing of custom-made Technology Assets, Applications and/or Services (TAAS).	SA-11(5)	SA-11(5)	SA-11(5)	SA-11(5)	SA-11(05)	SA-11(05)	SA-11(05)	SA-11(05)	SA-11(5)	SA-11(5)	SA-11(5)	SA-11(5)	SA-11(5)					
SA	SA-11(05)	SA-11(5)	Developer Testing and Evaluation | Penetration Testing	testing: a. At the following level of rigor: [Assignment:	SA-11(5)	Not Selected	Functional	Intersects With	5	Cybersecurity & Data Protection Testing Throughout Development	TDA-09	(1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified	SA-11(5)	SA-11(5)	SA-11(5)	SA-11(5)	SA-11(05)	SA-11(05)	SA-11(05)	SA-11(05)	SA-11(5)	SA-11(5)	SA-11(5)	SA-11(5)	SA-11(5)					
SA	SA-11(05)	SA-11(5)	Developer Testing and Evaluation | Penetration Testing	testing: a. At the following level of rigor: [Assignment:	SA-11(5)	Not Selected	Functional	Intersects With	5	Specialized Assessments	IAO-02.2	(5) Application security; (6) Embedded technologies (e.g., IoT, OT, etc.);	SA-11(5)	SA-11(5)	SA-11(5)	SA-11(5)	SA-11(05)	SA-11(05)	SA-11(05)	SA-11(05)	SA-11(5)	SA-11(5)	SA-11(5)	SA-11(5)	SA-11(5)					
SA	SA-11(05)	SA-11(5)	Developer Testing and Evaluation | Penetration Testing	testing: a. At the following level of rigor: [Assignment:	SA-11(5)	Not Selected	Functional	Intersects With	5	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	SA-11(5)	SA-11(5)	SA-11(5)	SA-11(5)	SA-11(05)	SA-11(05)	SA-11(05)	SA-11(05)	SA-11(5)	SA-11(5)	SA-11(5)	SA-11(5)	SA-11(5)					
SA	SA-11(06)	SA-11(6)	Developer Testing and Evaluation | Attack Surface Reviews	Analyze the developer's attack surface	SA-11(6)	Not Selected	Functional	Intersects With	5	Cybersecurity & Data Protection Testing Throughout Development	TDA-09	(1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified	SA-11(6)	SA-11(6)	SA-11(6)	SA-11(6)	SA-11(06)	SA-11(06)	SA-11(06)	SA-11(06)	SA-11(6)	SA-11(6)	SA-11(6)	SA-11(6)	SA-11(6)					
SA	SA-11(06)	SA-11(6)

Family	Sorting Control #	Focal Document Element	Focal Document Element Name	Focal Document Element Description	NIST SP 800-53 R5.2	Security Control Baseline	Set Theory Relationship Mapping (STRM)			Reference Document Element	Reference Document Name	Reference Document Element Description	NIST SP 800-53 R5.2 Baselines				FedRAMP R5				NIST SP 800-161 R1					GovRAMP				
							Rationale	Relationship	Strength of Relationship				Low	Mod	High	Privacy	Low	Mod	High	LI-SaaS	C-SCRM Baseline	Moderate Down Level 1	Level 1	Level 2	Level 3	Low	Low+	Moderate	Core	High (FedRAMP Rev 5)
SA	SA-12(06)	SA-12(6)		Withdrawn	SA-12(6)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
SA	SA-12(07)	SA-12(7)		Withdrawn	SA-12(7)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
SA	SA-12(08)	SA-12(8)		Withdrawn	SA-12(8)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
SA	SA-12(09)	SA-12(9)		Withdrawn	SA-12(9)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
SA	SA-12(10)	SA-12(10)		Withdrawn	SA-12(10)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
SA	SA-12(11)	SA-12(11)		Withdrawn	SA-12(11)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
SA	SA-12(12)	SA-12(12)		Withdrawn	SA-12(12)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
SA	SA-12(13)	SA-12(13)		Withdrawn	SA-12(13)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
SA	SA-12(14)	SA-12(14)		Withdrawn	SA-12(14)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
SA	SA-12(15)	SA-12(15)		Withdrawn	SA-12(15)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
SA	SA-13	SA-13		Withdrawn	SA-13	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
SA	SA-14	SA-14		Withdrawn	SA-14	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
SA	SA-14(01)	SA-14(1)		Withdrawn	SA-14(1)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
SA	SA-15	SA-15	Development Process, Standards, and Tools	Document, manage, and ensure the integrity of changes to the process and/or tools used in [Assignment: organization-defined development processes and/or tools]. Ensure the development processes and/or tools used in development are documented and managed. Require developers to identify and document planned remediation actions to correct weaknesses or deficiencies noted during the assessment of the developer's proposed or delivered flaw remediation process. Require developers to perform threat modeling and vulnerability analysis during development and the subsequent testing and evaluation of the system, component, or service that describes: A. The system, component, or service in its intended environment; and B. The threats considered and the methods used to determine the set of threats considered to be relevant based on the defined sources of threat information. Require developers to perform a criticality analysis at organization-defined decision points in the system development life cycle.	SA-15	Moderate	Functional	Equal	10	Secure Coding	TDA-06	Mechanisms exist to develop applications based on secure coding principles.		SA-15	SA-15			SA-15	SA-15				SA-15	SA-15						SA-15
SA	SA-15(01)	SA-15(1)	Development Process, Standards, and Tools | Quality Metrics	Provide evidence of meeting the quality metrics [Assignment: organization-defined quality metrics]. Require the developer of the system, component, or system service to select and employ security and privacy tracking tools for use during the development process.	SA-15(1)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SA	SA-15(02)	SA-15(2)	Development Process, Standards, and Tools | Criticality Analysis	Require the developer of the system, component, or system service to perform a criticality analysis at [Assignment: organization-defined decision points in the system development life cycle].	SA-15(2)	Not Selected	Functional	Equal	10	Plan of Action & Milestones (POA&M)	IAO-05	Mechanisms exist to require the developer of the Technology Asset, Application and/or Service (TAAS) to perform a criticality analysis at organization-defined decision points in the Secure Development Life		SA-15(3)	SA-15(3)			SA-15(03)	SA-15(03)				SA-15(3)	SA-15(3)						
SA	SA-15(03)	SA-15(3)	Development Process, Standards, and Tools | Criticality Analysis		SA-15(3)	Moderate	Functional	Equal	10	Criticality Analysis	TDA-06.1													SA-15(3)	SA-15(3)					
SA	SA-15(04)	SA-15(4)		Withdrawn	SA-15(4)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A												SA-15(4)	SA-15(4)					
SA	SA-15(05)	SA-15(5)	Development Process, Standards, and Tools | Attack Surface Reduction	Reduce the attack surface of the system, system component, or system service to reduce attack surfaces to meet [Assignment: organization-defined requirements]. Require the developer of the system, system component, or system service to reduce attack surfaces to meet [Assignment: organization-defined requirements].	SA-15(5)	Not Selected	Functional	Intersects With	5	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system	SA-15(5)	SA-15(5)	SA-15(5)	SA-15(5)	SA-15(05)	SA-15(05)	SA-15(05)	SA-15(05)	SA-15(5)	SA-15(5)	SA-15(5)	SA-15(5)	SA-15(5)					
SA	SA-15(05)	SA-15(5)	Development Process, Standards, and Tools | Attack Surface Reduction		SA-15(5)	Not Selected	Functional	Intersects With	5	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity and data protection practices in the specification, design, development, implementation and modification of	SA-15(5)	SA-15(5)	SA-15(5)	SA-15(5)	SA-15(05)	SA-15(05)	SA-15(05)	SA-15(05)	SA-15(5)	SA-15(5)	SA-15(5)	SA-15(5)	SA-15(5)					
SA	SA-15(06)	SA-15(6)	Development Process, Standards, and Tools | Continuous Improvement	Implement an explicit process to continuously improve the development component, or system service to implement an explicit process to continuously improve the development organization-defined tools]. Determine the exploitation potential for discovered vulnerabilities. Determine potential, or discovered vulnerabilities. Determine exploitation potential for discovered vulnerabilities. Determine	SA-15(6)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SA	SA-15(07)	SA-15(7)	Development Process, Standards, and Tools | Automated Vulnerability Analysis	and vulnerability analyses from similar systems,	SA-15(7)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SA	SA-15(08)	SA-15(8)	Development Process, Standards, and Tools | Reuse of Threat and Vulnerability Information	and vulnerability analyses from similar systems, within the system to inform the current	SA-15(8)	Not Selected	Functional	Equal	10	Threat Modeling	TDA-06.2	Mechanisms exist to perform threat modeling and other secure design techniques, to ensure that threats to software and solutions are identified and accounted for.													SA-15(8)					
SA	SA-15(09)	SA-15(9)		Withdrawn	SA-15(9)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
SA	SA-15(10)	SA-15(10)	Development Process, Standards, and Tools | Incident Response Plan	Provide the developer of the system, system component, or system service with a copy of the incident response plan for the system or system component to be released or delivered together with the corresponding system or system component. Require the developer of the system, system component to minimize the use of personally identifiable information to design, develop, and implement only the organization-defined personally identifiable information (PII) [Assignment: organization-defined PII].	SA-15(10)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SA	SA-15(11)	SA-15(11)	Development Process, Standards, and Tools | Archive System or Component		SA-15(11)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SA	SA-15(12)	SA-15(12)	Development Process, Standards, and Tools | Minimize Personally Identifiable Information		SA-15(12)	Not Selected	Functional	Equal	10	Limit Sensitive / Regulated Data In Testing, Training & Research	DCH-18.2	Mechanisms exist to minimize the use of sensitive/regulated data for research, testing, or training, in accordance with authorized, legitimate business practices																		
SA	SA-15(13)	SA-15(13)	Development Process, Standards, and Tools | Logging Syntax	Require the developer of the system, system component, or system service to use an [Assignment: organization-defined secure logging format] to log	SA-15(13)	Not Selected	Functional	Equal	10	Logging Syntax	TDA-02.14	Mechanisms exist to require system developers to use an industry-defined secure logging format to generate event logs for specified event types at organization-defined level of detail.																		
SA	SA-16	SA-16	Developer-provided Training	Require the developer of the system, system component, or system service to provide [Assignment: organization-defined training] on the correct use and operation of the implemented security and privacy functions, controls,	SA-16	High	Functional	Equal	10	Developer-Provided Training	TDA-16	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to provide training on the correct use and operation of the Technology Asset, Application and/or Service			SA-16				SA-16				SA-16	SA-16						SA-16
SA	SA-17	SA-17	Developer Security and Privacy Architecture and Design	Require the developer of the system, system component, or system service to: A. Produce a design specification and security architecture that: B. Is consistent with the organization's enterprise architecture that addresses risk; C. Accurately and completely describes the required security and privacy functionality, and the allocation of controls among physical and logical components; and D. Expresses how individual hardware, software, and firmware security functions interact and how they relate to the overall system security architecture; and E. Describe the design and implementation of controls that address the security and privacy requirements.	SA-17	High	Functional	Equal	10	Developer Architecture & Design	TDA-05	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to produce a design specification and security architecture that:			SA-17				SA-17				SA-17	SA-17						SA-17
SA	SA-17(01)	SA-17(1)	Developer Security and Privacy Architecture and Design | Formal Policy Model	Require the developer to: A. Produce, as an input to the system, a formal policy model, as an informal explanation of the system behavior with respect to [Assignment: organization-defined elements of organizational security and privacy policy] to be enforced; and B. Define the relevant elements of the formal policy model;	SA-17(1)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SA	SA-17(02)	SA-17(2)	Developer Security and Privacy Architecture and Design | Security-relevant Components	Require the developer to: A. Define the security-relevant hardware, software, and firmware; and B. Provide a rationale that the definition for security-relevant hardware, software, and firmware is complete.	SA-17(2)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SA	SA-17(03)	SA-17(3)	Developer Security and Privacy Architecture and Design | Formal Correspondence	Require the developer to: A. Produce, as an input to the system, a formal top-level specification that is consistent with the formal policy model; B. Show via [Selection (one): informal demonstration, that the descriptive top-level specification is consistent with the formal policy model; C. Show via informal demonstration, that the descriptive	SA-17(3)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SA	SA-17(04)	SA-17(4)	Developer Security and Privacy Architecture and Design | Informal Correspondence	Show via informal demonstration, that the descriptive top-level specification is consistent with the formal policy model; C. Show via informal demonstration, that the descriptive	SA-17(4)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SA	SA-17(05)	SA-17(5)	Developer Security and Privacy Architecture and Design | Conceptually Simple Design	Require the developer to: A. Design and structure the system to use a complete, conceptually simple protection mechanism with precisely defined semantics; and B. Internally structure the system to	SA-17(5)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SA	SA-17(06)	SA-17(6)	Developer Security and Privacy Architecture and Design | Structure for Testing	Require the developer to structure the system component, or system service to structure security-relevant hardware, software, and firmware to facilitate	SA-17(6)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SA	SA-17(07)	SA-17(7)	Developer Security and Privacy Architecture and Design | Structure for Least Privilege	Require the developer to structure the system component, or system service to structure security-relevant hardware, software, and firmware to facilitate	SA-17(7)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SA	SA-17(08)	SA-17(8)	Developer Security and Privacy Architecture and Design | Orchestration	Require the developer to implement the following capabilities: [Assignment: organization-defined capabilities]; and Design, implement, and orchestrate [Assignment: organization-defined mechanisms] to	SA-17(8)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SA	SA-17(09)	SA-17(9)	Developer Security and Privacy Architecture and Design | Design Diversity	Require the developer to: A. Design and structure the system to use a complete, conceptually simple protection mechanism with precisely defined semantics; and B. Internally structure the system to	SA-17(9)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SA	SA-18	SA-18		Withdrawn	SA-18	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
SA	SA-18(01)	SA-18(1)		Withdrawn	SA-18(1)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
SA	SA-18(02)	SA-18(2)		Withdrawn	SA-18(2)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
SA	SA-19	SA-19		Withdrawn	SA-19	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
SA	SA-19(01)	SA-19(1)		Withdrawn	SA-19(1)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
SA	SA-19(02)	SA-19(2)		Withdrawn	SA-19(2)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
SA	SA-19(03)	SA-19(3)		Withdrawn	SA-19(3)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
SA	SA-19(04)	SA-19(4)		Withdrawn	SA-19(4)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
SA	SA-20	SA-20	Customized Development of Critical Components	Reimplement or custom develop [Assignment: organization-defined critical system components]. Reimplement or custom develop critical system components, when Commercial Off The Shelf (COTS) solutions are unavailable.	SA-20	Not Selected	Functional	Equal	10	Customized Development of Critical Components	TDA-12	Mechanisms exist to custom-develop critical system components, when Commercial Off The Shelf (COTS) solutions are unavailable.											SA-20	SA-20					
SA	SA-21	SA-21	Developer Screening	Require that the developer of [Assignment: organization-defined system, system component, or system service] meet [Assignment: organization-defined personnel screening criteria]. Require that the developer of [Assignment: organization-defined system, system component, or system service] meet [Assignment: organization-defined official government duties]; and b. Satisfies the	SA-21	High	Functional	Equal	10	Developer Screening	TDA-13	Mechanisms exist to ensure that the developers of Technology Assets, Applications and/or Services (TAAS) have the requisite skillset and appropriate access authorizations.				SA-21			SA-21		SA-21		SA-21	SA-21						
SA	SA-21(01)	SA-21(1)		Withdrawn	SA-21(1)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A												SA-21(1)	SA-21(1)					
SA	SA-22	SA-22	Unsupported System Components	Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; and Provide the following options for alternative sources for continued support for	SA-22	Low	Functional	Intersects With	5	Unsupported Technology Assets, Applications and/or Services (TAAS)	TDA-17	(1) Removing and/or replacing TAAS when support for the components is no longer available from the	SA-22	SA-22	SA-22	SA-22	SA-22	SA-22	SA-22	SA-22	SA-22	SA-22	SA-22	SA-22	SA-22					
SA	SA-22	SA-22	Unsupported System Components	options for alternative sources for continued support for	SA-22	Low	Functional	Intersects With	5	Alternate Sources for Continued Support	TDA-17.1	Mechanisms exist to provide in-house support or contract external providers for support with unsupported Technology Assets, Applications and/or Services (TAAS).	SA-22	SA-22	SA-22	SA-22	SA-22	SA-22	SA-22	SA-22	SA-22	SA-22	SA-22	SA-22	SA-22					
SA	SA-22(01)	SA-22(1)		Withdrawn	SA-22(1)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
SA	SA-23	SA-23	Specialization	Require the developer of [Assignment: organization-defined systems or system components] supporting mission essential services or functions to	SA-23	Not Selected	Functional	Intersects With	5	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	SA-23	SA-23	SA-23	SA-23	SA-23	SA-23	SA-23	SA-23	SA-23	SA-23	SA-23	SA-23	SA-23					
SA	SA-23	SA-23	Specialization	Require the developer of [Assignment: organization-defined systems or system components] supporting mission essential services or functions to	SA-23	Not Selected	Functional	Intersects With	5	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across	SA-23	SA-23	SA-23	SA-23	SA-23	SA-23	SA-23	SA-23	SA-23	SA-23	SA-23	SA-23	SA-23					
SA	SA-23	SA-23	Specialization	Require the developer of [Assignment: organization-defined systems or system components] supporting mission essential services or functions to	SA-23	Not Selected	Functional	Intersects With	5	Customized Development of Critical Components	TDA-12	Mechanisms exist to custom-develop critical system components, when Commercial Off The Shelf (COTS) solutions are unavailable.	SA-23	SA-23	SA-23	SA-23	SA-23	SA-23	SA-23	SA-23	SA-23	SA-23	SA-23	SA-23	SA-23					
SC	SC-01	SC-1	Policy and Procedures	Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: A. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and communications protection policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and B. Procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection	SC-1	Low	Functional	Intersects With	5	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	SC-1	SC-1	SC-1	SC-1	SC-01	SC-01	SC-01	SC-01	SC-1	SC-1	SC-1	SC-1	SC-1	SC-01	SC-01	SC-01	SC-01
SC	SC-01	SC-1	Policy and Procedures	Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: A. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and communications protection policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and B. Procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection	SC-1	Low	Functional	Subset Of	10	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	SC-1	SC-1	SC-1	SC-1	SC-01	SC-01	SC-01	SC-01	SC-1	SC-1	SC-1	SC-1	SC-1	SC-01	SC-01	SC-01	SC-01
SC	SC-01	SC-1	Policy and Procedures	Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: A. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and communications protection policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and B. Procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection	SC-1	Low	Functional	Subset Of	10	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity and data protection practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	SC-1	SC-1	SC-1	SC-1	SC-01	SC-01	SC-01	SC-01	SC-1	SC-1	SC-1	SC-1	SC-1	SC-01	SC-01	SC-01	SC-01
SC	SC-01	SC-1	Policy and Procedures	Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: A. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and communications protection policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and B. Procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection	SC-1	Low	Functional	Intersects With	5	Cybersecurity & Data Protection Governance Program	GOV-03	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures, at planned intervals or if significant changes occur to ensure their	SC-1	SC-1	SC-1	SC-1	SC-01	SC-01	SC-01	SC-01	SC-1	SC-1	SC-1	SC-1	SC-1	SC-01	SC-01	SC-01	SC-01
SC	SC-02	SC-2	Separation of System and User Functionality	Separate user functionality, including user interface services, from system management functionality.	SC-2	Moderate	Functional	Equal	10	Application Partitioning	SEA-03.2	Mechanisms exist to separate user functionality from system management functionality.		SC-2	SC-2			SC-02	SC-02								SC-02	SC-02	SC-02	SC-02
SC	SC-02(01)	SC-2(1)	Separation of System and User Functionality | Interfaces for Non-privileged Users	Prevent the presentation of system management functionality at interfaces to non-privileged users.	SC-2(1)	Not Selected	Functional	Equal	10	Application Partitioning	SEA-03.2	Mechanisms exist to separate user functionality from system management functionality.																		
SC	SC-02(02)	SC-2(2)	Separation of System and User Functionality | Disassociability	Store state information from applications and software separately.	SC-2(2)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SC	SC-03	SC-3	Security Function Isolation	Isolate security functions from nonsecurity functions.	SC-3	High	Functional	Intersects With	5	Restrict Access To Security Functions	END-16	Mechanisms exist to ensure security functions are restricted to authorized individuals and enforce least privilege control requirements for necessary job functions.	SC-3	SC-3	SC-3	SC-3	SC-03	SC-03	SC-03	SC-03	SC-3	SC-3	SC-3	SC-3	SC-3					SC-03
SC	SC-03	SC-3	Security Function Isolation	Isolate security functions from nonsecurity functions.	SC-3	High	Functional	Intersects With	5	Security Function Isolation	SEA-04.1	Mechanisms exist to isolate security functions from non-security functions.	SC-3	SC-3	SC-3	SC-3	SC-03	SC-03	SC-03	SC-03	SC-3	SC-3	SC-3	SC-3	SC-3					SC-03
SC	SC-03(01)	SC-3(1)	Security Function Isolation | Hardware Separation	Employ hardware separation mechanisms to implement security function isolation.	SC-3(1)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SC	SC-03(02)	SC-3(2)	Security Function Isolation | Access and Flow Control Functions	Isolate security functions enforcing access and information flow control from nonsecurity functions and from other security functions.	SC-3(2)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SC	SC-03(03)	SC-3(3)	Security Function Isolation | Minimize Nonsecurity Functionality	Minimize the nonsecurity functionality in the isolation boundary containing security functions.	SC-3(3)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SC	SC-03(04)	SC-3(4)	Security Function Isolation | Module Coupling and Cohesiveness	Implement security function as modular code. Maintain the following system security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or	SC-3(4)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SC	SC-03(05)	SC-3(5)	Security Function Isolation | Layered Structures	minimizing interactions between layers of the design and avoiding any dependence by lower layers on the	SC-3(5)	Not Selected	Functional	Equal	10	Defense-in-Depth (DID) Architecture	SEA-03	between layers of the design and avoiding any dependence by lower layers on the functionality or																		
SC	SC-04	SC-4	Information in Shared System Resources	Prevent unauthorized and unintended information transfer via shared system resources.	SC-4	Moderate	Functional	Equal	10	Information In Shared Resources	SEA-05	Mechanisms exist to prevent unauthorized and unintended information transfer via shared system resources.		SC-4	SC-4			SC-04	SC-04				SC-4	SC-4			SC-04	SC-04	SC-04	SC-04
SC	SC-04(01)	SC-4(1)		Withdrawn	SC-4(1)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
SC	SC-04(02)	SC-4(2)	Information in Shared System Resources | Multilevel or Periods Processing	Prevent unauthorized and unintended information transfer via shared system resources. Prevent unauthorized and unintended information transfer via shared system resources.	SC-4(2)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SC	SC-05	SC-5	Denial-of-service Protection	Provide [Assignment: organization-defined controls] by [Assignment: organization-defined procedures] when system processing explicitly [Assignment: organization-defined controls] by [Assignment: organization-defined procedures] when system processing explicitly	SC-5	Low	Functional	Intersects With	5	Resource Priority	CAP-02	Mechanisms exist to control resource utilization of Technology Assets, Applications and/or Services (TAAS) that are susceptible to Denial of Service (DoS) attacks to limit and prioritize the use of	SC-5	SC-5	SC-5	SC-5	SC-05	SC-05	SC-05	SC-05	SC-5	SC-5	SC-5	SC-5	SC-5	SC-05	SC-05	SC-05	SC-05
SC	SC-05	SC-5	Denial-of-service Protection	service events]; and b. Employ the following controls to service events]; and b. Employ the following controls to	SC-5	Low	Functional	Intersects With	5	Capacity Planning	CAP-03	Mechanisms exist to conduct capacity planning so that necessary capacity for information processing, telecommunications and environmental support will exist during contingency operations.	SC-5	SC-5	SC-5	SC-5	SC-05	SC-05	SC-05	SC-05	SC-5	SC-5	SC-5	SC-5	SC-5	SC-05	SC-05	SC-05	SC-05
SC	SC-05	SC-5	Denial-of-service Protection	protect from organization-defined types of denial-of-service events]; and b. Employ the following controls to protect from organization-defined types of denial-of-service	SC-5	Low	Functional	Intersects With	5	Capacity & Performance Management	CAP-01	Mechanisms exist to facilitate the implementation of capacity management controls to ensure optimal system performance to meet expected and anticipated future capacity requirements.	SC-5	SC-5	SC-5	SC-5	SC-05	SC-05	SC-05	SC-05	SC-5	SC-5	SC-5	SC-5	SC-5	SC-05	SC-05	SC-05	SC-05
SC	SC-05	SC-5	Denial-of-service Protection	protect from organization-defined types of denial-of-service events]; and b. Employ the following controls to protect from organization-defined types of denial-of-service	SC-5	Low	Functional	Intersects With	5	Denial of Service (DoS) Protection	NET-02.1	Automated mechanisms exist to protect against or limit the effects of denial of service attacks.	SC-5	SC-5	SC-5	SC-5	SC-05	SC-05	SC-05	SC-05	SC-5	SC-5	SC-5	SC-5	SC-5	SC-05	SC-05	SC-05	SC-05
SC	SC-05(01)	SC-5(1)	Denial-of-service Protection | Restrict Ability to Attack Other Systems	Restrict the ability of individuals to launch denial-of-service attacks against other systems. Restrict the ability of individuals to launch denial-of-service	SC-5(1)	Not Selected	Functional	Intersects With	5	Resource Priority	CAP-02	Mechanisms exist to control resource utilization of Technology Assets, Applications and/or Services (TAAS) that are susceptible to Denial of Service (DoS) attacks to limit and prioritize the use of																				
SC	SC-05(02)	SC-5(2)	Denial-of-service Protection | Capacity, Bandwidth, and Redundancy	Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding denial-of-service	SC-5(2)	Not Selected	Functional	Intersects With	5	Resource Priority	CAP-02	Mechanisms exist to control resource utilization of Technology Assets, Applications and/or Services (TAAS) that are susceptible to Denial of Service (DoS) attacks to limit and prioritize the use of	SC-5(2)	SC-5(2)	SC-5(2)	SC-5(2)	SC-05(02)	SC-05(02)	SC-05(02)	SC-05(02)	SC-5(2)	SC-5(2)	SC-5(2)	SC-5(2)	SC-5(2)					
SC	SC-05(02)	SC-5(2)	Denial-of-service Protection | Capacity, Bandwidth, and Redundancy	Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding denial-of-service	SC-5(2)	Not Selected	Functional	Intersects With	5	Capacity Planning	CAP-03	Mechanisms exist to conduct capacity planning so that necessary capacity for information processing, telecommunications and environmental support will exist during contingency operations.	SC-5(2)	SC-5(2)	SC-5(2)	SC-5(2)	SC-05(02)	SC-05(02)	SC-05(02)	SC-05(02)	SC-5(2)	SC-5(2)	SC-5(2)	SC-5(2)	SC-5(2)					
SC	SC-05(03)	SC-5(3)	Denial-of-service Protection | Detection and Monitoring	Employ the following monitoring tools: [Assignment: organization-defined monitoring tools]; and Incorporate the following information into the [Assignment: organization-defined resources] by [Selection (one or more): priority; quota; [Assignment:	SC-5(3)	Not Selected	Functional	Intersects With	5	Capacity & Performance Management	CAP-01	Mechanisms exist to facilitate the implementation of capacity management controls to ensure optimal system performance to meet expected and anticipated future capacity requirements.																		
SC	SC-06	SC-6	Resource Availability	Protect the availability of resources by [Assignment: organization-defined resources] by [Selection (one or more): priority; quota; [Assignment:	SC-6	Not Selected	Functional	Intersects With	5	Resource Priority	CAP-02	Mechanisms exist to control resource utilization of Technology Assets, Applications and/or Services (TAAS) that are susceptible to Denial of Service (DoS) attacks to limit and prioritize the use of																		
SC	SC-07	SC-7	Boundary Protection	Monitor and control communications at the external boundary of the system and at key internal boundaries within the system; Implement subnetworks for publicly accessible system components that are [Selection (one): physically; logically] separated from internal organizational networks; and c. Connect to	SC-7	Low	Functional	Intersects With	5	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	SC-7	SC-7	SC-7		SC-07	SC-07	SC-07	SC-07	SC-7	SC-7		SC-7		SC-07	SC-07	SC-07	SC-07	SC-07
SC	SC-07(01)	SC-7(1)		Withdrawn	SC-7(1)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
SC	SC-07(02)	SC-7(2)		Withdrawn	SC-7(2)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
SC	SC-07(03)	SC-7(3)	Boundary Protection | Access Points	Limit the number of external network connections to the system.	SC-7(3)	Moderate	Functional	Equal	10	Limit Network Connections	NET-03.1	Mechanisms exist to limit the number of concurrent external network connections to its Technology Assets, Applications and/or Services (TAAS).			SC-7(3)	SC-7(3)			SC-07(03)	SC-07(03)										SC-07(03)	SC-07

Family	Sorting Control #	Focal Document Element	Focal Document Element Name	Focal Document Element Description	NIST SP 800-53 R5.2	Security Control Baseline	Set Theory Relationship Mapping (STRM) Rationale	Relationship	Strength of Relationship	Reference Document Element	Reference Document Element Name	Reference Document Element Description	NIST SP 800-53 R5.2 Baselines Low	Mod	High	Privacy	FedRAMP R5 Low	Mod	High	LI-SaaS	NIST SP 800-161 R1 C-SCRM Baseline	Moderate Impact-level Open Source Overlay	Level 1	Level 2	Level 3	GovRAMP Low	Low+	Moderate	Core	High (FedRAMP Rev. 5)
SC	SC-07(11)	SC-7(11)	Boundary Protection | Restrict Incoming Communications Traffic	[Assignment: organization-defined authorized sources] to be routed to [Assignment: organization-defined authorized processing devices]	SC-7(11)	Not Selected	Functional	Intersects With	5	Deny Traffic by Default & Allow Traffic by Exception	NET-04.1	Mechanisms exist to configure firewall and router configurations to deny network traffic by default and allow network traffic by exception (e.g., deny all, permit by exception).	SC-7(11)	SC-7(11)	SC-7(11)	SC-7(11)	SC-07(11)	SC-07(11)	SC-07(11)	SC-07(11)	SC-7(11)	SC-7(11)	SC-7(11)	SC-7(11)	SC-7(11)					
SC	SC-07(11)	SC-7(11)	Boundary Protection | Restrict Incoming Communications Traffic	[Assignment: organization-defined authorized sources] to be routed to [Assignment: organization-defined authorized processing devices]	SC-7(11)	Not Selected	Functional	Intersects With	5	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	SC-7(11)	SC-7(11)	SC-7(11)	SC-7(11)	SC-07(11)	SC-07(11)	SC-07(11)	SC-07(11)	SC-7(11)	SC-7(11)	SC-7(11)	SC-7(11)	SC-7(11)					
SC	SC-07(12)	SC-7(12)	Boundary Protection | Host-based Protection	[Assignment: organization-defined host-based boundary protection mechanisms] at [Assignment: organization-defined information system components]	SC-7(12)	Not Selected	Functional	Equal	10	Host-Based Security Function Isolation	END-16.1	Mechanisms exist to implement underlying software separation mechanisms to facilitate security function isolation.						SC-07(12)	SC-07(12)							SC-07(12)	SC-07(12)		SC-07(12)
SC	SC-07(13)	SC-7(13)	Boundary Protection | Isolation of Security Tools, Mechanisms, and Support Components	Isolate [Assignment: organization-defined information security tools, mechanisms, and support components] from other internal system components by implementing [Assignment: organization-defined physical and/or logical isolation boundaries]	SC-7(13)	Not Selected	Functional	Intersects With	5	Security Management Subnets	NET-06.1	Mechanisms exist to implement security management subnets to isolate security tools and support components from other internal system components by implementing separate subnetworks with managed interfaces to other components of the system.									SC-7(13)			SC-7(13)		SC-07(13)	SC-07(13)		SC-07(13)
SC	SC-07(14)	SC-7(14)	Boundary Protection | Protect Against Unauthorized Physical Connections	Protect against unauthorized physical connections at [Assignment: organization-defined managed interfaces]	SC-7(14)	Not Selected	Functional	Intersects With	5	Equipment Siting & Protection	PES-12	Physical security mechanisms exist to locate system components within the facility to minimize the opportunity for unauthorized access or potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.	SC-7(14)	SC-7(14)	SC-7(14)	SC-7(14)	SC-07(14)	SC-07(14)	SC-07(14)	SC-07(14)	SC-7(14)	SC-7(14)	SC-7(14)	SC-7(14)	SC-7(14)					
SC	SC-07(14)	SC-7(14)	Boundary Protection | Protect Against Unauthorized Physical Connections	Protect against unauthorized physical connections at [Assignment: organization-defined managed interfaces]	SC-7(14)	Not Selected	Functional	Intersects With	5	Lockable Physical Casings	PES-03.2	Physical access control mechanisms exist to protect system components from unauthorized physical access (e.g., lockable physical casings).	SC-7(14)	SC-7(14)	SC-7(14)	SC-7(14)	SC-07(14)	SC-07(14)	SC-07(14)	SC-07(14)	SC-7(14)	SC-7(14)	SC-7(14)	SC-7(14)	SC-7(14)					
SC	SC-07(14)	SC-7(14)	Boundary Protection | Protect Against Unauthorized Physical Connections	Protect against unauthorized physical connections at [Assignment: organization-defined managed interfaces]	SC-7(14)	Not Selected	Functional	Intersects With	5	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	SC-7(14)	SC-7(14)	SC-7(14)	SC-7(14)	SC-07(14)	SC-07(14)	SC-07(14)	SC-07(14)	SC-7(14)	SC-7(14)	SC-7(14)	SC-7(14)	SC-7(14)					
SC	SC-07(15)	SC-7(15)	Boundary Protection | Networked Privileged Accesses	Route networked, privileged accesses through a dedicated, managed interface for purposes of access control and auditing	SC-7(15)	Not Selected	Functional	Equal	10	Route Privileged Network Access	NET-18.3	Automated mechanisms exist to route networked, privileged accesses through a dedicated, managed interface for purposes of access control and auditing.																		
SC	SC-07(16)	SC-7(16)	Boundary Protection | Prevent Discovery of System Components	Prevent the discovery of specific system components that represent a managed interface.	SC-7(16)	Not Selected	Functional	Equal	10	Prevent Discovery of Internal Information	NET-03.3	Mechanisms exist to prevent the public disclosure of internal network information.																		
SC	SC-07(17)	SC-7(17)	Boundary Protection | Automated Enforcement of Protocol Formats	Enforce adherence to protocol formats.	SC-7(17)	Not Selected	Functional	Equal	10	Web Application Firewall (WAF)	WEB-03	Mechanisms exist to deploy Web Application Firewalls (WAFs) to provide defense-in-depth protection for application-specific threats.																		
SC	SC-07(18)	SC-7(18)	Boundary Protection | Fail Secure	Prevent systems from entering unknown or unsecure states in the event of an operational failure of a boundary protection device.	SC-7(18)	High	Functional	Equal	10	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity and data protection practices in the specification, design, development, implementation and modification of systems and services.			SC-7(18)			SC-07(18)	SC-07(18)								SC-07(18)		SC-07(18)	SC-07(18)
SC	SC-07(19)	SC-7(19)	Boundary Protection | Block Communication from Non-organizationally Configured Hosts	Block inbound and outbound communications traffic between [Assignment: organization-defined communications] that are independently configured by end users and external service providers.	SC-7(19)	Not Selected	Functional	Intersects With	5	Network Access Control (NAC)	AST-02.5	Automated mechanisms exist to enforce Network Access Control (NAC) using endpoint security validation and compliance tools or agents that verify the endpoint device is compliant with security configuration requirements prior to allowing the device to connect to the network.											SC-7(19)							
SC	SC-07(20)	SC-7(20)	Boundary Protection | Dynamic Isolation and Segregation	Provide the capability to dynamically isolate [Assignment: organization-defined system components] from other system components.	SC-7(20)	Not Selected	Functional	Equal	10	Dynamic Isolation & Segregation (Sandboxing)	NET-03.6	Mechanisms exist to employ dynamic isolation & segregation (sandboxing) capabilities to limit the impact of potentially-malicious or compromised software or data by executing it in a restricted execution environment (e.g., sandbox, virtualized environment, container) or prevent it from executing outside of the restricted execution environment (e.g., "air gapping" the system hosting the software or data).						SC-07(20)												
SC	SC-07(21)	SC-7(21)	Boundary Protection | Isolation of System Components	Employ boundary protections to isolate [Assignment: organization-defined system components] supporting [Assignment: organization-defined missions and/or business functions].	SC-7(21)	High	Functional	Equal	10	Isolation of System Components	NET-03.7	Mechanisms exist to employ boundary protections to isolate Technology Assets, Applications and/or Services (TAAS) that support critical missions and/or business functions.			SC-7(21)			SC-07(21)												SC-07(21)
SC	SC-07(22)	SC-7(22)	Boundary Protection | Separate Subnets for Connecting to Different Security Domains	Implement separate network addresses to connect to systems in different security domains.	SC-7(22)	Not Selected	Functional	Intersects With	5	Separate Subnet for Connecting to Different Security Domains	NET-03.8	Mechanisms exist to implement separate network addresses (e.g., different subnets) to connect to systems in different security domains.																		
SC	SC-07(23)	SC-7(23)	Boundary Protection | Disable Sender Feedback on Protocol Validation Failure	Disable feedback to senders on protocol format validation failure.	SC-7(23)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SC	SC-07(24)	SC-7(24)	Boundary Protection | Personally Identifiable Information	Monitor for permitted processing at the external interfaces to [Assignment: organization-defined unauthorized exchanges of personally identifiable information] and at [Assignment: organization-defined boundary protections] within the system.	SC-7(24)	Not Selected	Functional	Equal	10	Personal Data (PD)	NET-03.4	Mechanisms exist to apply network-based processing rules to data elements of Personal Data (PD).				SC-7(24)														
SC	SC-07(25)	SC-7(25)	Boundary Protection | Unclassified National Security System Connections	Prohibit the direct connection of [Assignment: organization-defined unclassified national security system] to an external network without the use of [Assignment: organization-defined boundary protection device].	SC-7(25)	Not Selected	Functional	Intersects With	5	System Interconnections	NET-05	Mechanisms exist to prohibit the direct connection of a sensitive system to an external network without the use of an organization-defined boundary protection device.																		
SC	SC-07(26)	SC-7(26)	Boundary Protection | Classified National Security System Connections	Prohibit the direct connection of [Assignment: organization-defined classified national security system] to an external network without the use of [Assignment: organization-defined boundary protection device].	SC-7(26)	Not Selected	Functional	Intersects With	5	System Interconnections	NET-05	Mechanisms exist to prohibit the direct connection of a sensitive system to an external network without the use of an organization-defined boundary protection device.																		
SC	SC-07(27)	SC-7(27)	Boundary Protection | Unclassified Non-national Security System Connections	Prohibit the direct connection of [Assignment: organization-defined unclassified non-national security system] to an external network without the use of [Assignment: organization-defined boundary protection device].	SC-7(27)	Not Selected	Functional	Equal	10	External System Connections	NET-05.1	Mechanisms exist to prohibit the direct connection of a sensitive system to an external network without the use of an organization-defined boundary protection device.																		
SC	SC-07(28)	SC-7(28)	Boundary Protection | Connections to Public Networks	Prohibit the direct connection of [Assignment: organization-defined system] to a public network.	SC-7(28)	Not Selected	Functional	Equal	10	Direct Internet Access Restrictions	NET-06.5	Mechanisms exist to prohibit, or strictly-control, Internet access from sensitive / regulated data enclaves (secure zones).																		
SC	SC-07(29)	SC-7(29)	Boundary Protection | Separate Subnets to Isolate Functions	Implement [Selection (one or more): physically; logically] separate subnets to isolate [Assignment: organization-defined system components and functions].	SC-7(29)	Not Selected	Functional	Intersects With	5	Cloud Infrastructure Security Subnet	CLD-03	Mechanisms exist to host security-specific technologies in a dedicated subnet.	SC-7(29)	SC-7(29)	SC-7(29)	SC-7(29)	SC-07(29)	SC-07(29)	SC-07(29)	SC-07(29)	SC-7(29)	SC-7(29)	SC-7(29)	SC-7(29)	SC-7(29)					
SC	SC-07(29)	SC-7(29)	Boundary Protection | Separate Subnets to Isolate Functions	Implement [Selection (one or more): physically; logically] separate subnets to isolate [Assignment: organization-defined system components and functions].	SC-7(29)	Not Selected	Functional	Equal	10	Security Management Subnets	NET-06.1	Mechanisms exist to implement security management subnets to isolate security tools and support components from other internal system components by implementing separate subnetworks with managed interfaces to other components of the system.	SC-7(29)	SC-7(29)	SC-7(29)	SC-7(29)	SC-07(29)	SC-07(29)	SC-07(29)	SC-07(29)	SC-7(29)	SC-7(29)	SC-7(29)	SC-7(29)	SC-7(29)					
SC	SC-07(29)	SC-7(29)	Boundary Protection | Separate Subnets to Isolate Functions	Implement [Selection (one or more): physically; logically] separate subnets to isolate [Assignment: organization-defined system components and functions].	SC-7(29)	Not Selected	Functional	Intersects With	5	Separate Subnet for Connecting to Different Security Domains	NET-03.8	Mechanisms exist to implement separate network addresses (e.g., different subnets) to connect to systems in different security domains.	SC-7(29)	SC-7(29)	SC-7(29)	SC-7(29)	SC-07(29)	SC-07(29)	SC-07(29)	SC-07(29)	SC-7(29)	SC-7(29)	SC-7(29)	SC-7(29)	SC-7(29)					
SC	SC-08	SC-8	Transmission Confidentiality and Integrity	Protect the [Selection (one or more): confidentiality; integrity] of transmitted information.	SC-8	Moderate	Functional	Intersects With	5	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	SC-8	SC-8	SC-8	SC-8	SC-08	SC-08	SC-08	SC-08	SC-8	SC-8	SC-8	SC-8	SC-8		SC-08	SC-08		SC-08
SC	SC-08	SC-8	Transmission Confidentiality and Integrity	Protect the [Selection (one or more): confidentiality; integrity] of transmitted information.	SC-8	Moderate	Functional	Intersects With	5	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	SC-8	SC-8	SC-8	SC-8	SC-08	SC-08	SC-08	SC-08	SC-8	SC-8	SC-8	SC-8	SC-8		SC-08	SC-08		SC-08
SC	SC-08(01)	SC-8(1)	Transmission Confidentiality and Integrity | Cryptographic Protection	Implement cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.	SC-8(1)	Moderate	Functional	Intersects With	5	Alternate Physical Protection	CRY-01.1	Cryptographic mechanisms exist to prevent unauthorized disclosure of information as an alternative to physical safeguards.	SC-8(1)	SC-8(1)	SC-8(1)	SC-8(1)	SC-08(01)	SC-08(01)	SC-08(01)	SC-08(01)	SC-8(1)	SC-8(1)	SC-8(1)	SC-8(1)	SC-8(1)			SC-08(01)		SC-08(01)
SC	SC-08(01)	SC-8(1)	Transmission Confidentiality and Integrity | Cryptographic Protection	Implement cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.	SC-8(1)	Moderate	Functional	Intersects With	5	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	SC-8(1)	SC-8(1)	SC-8(1)	SC-8(1)	SC-08(01)	SC-08(01)	SC-08(01)	SC-08(01)	SC-8(1)	SC-8(1)	SC-8(1)	SC-8(1)	SC-8(1)			SC-08(01)		SC-08(01)
SC	SC-08(02)	SC-8(2)	Transmission Confidentiality and Integrity | Pre- and Post-transmission Handling	Maintain the [Selection (one or more): confidentiality; integrity] of information during preparation for transmission and during reception.	SC-8(2)	Not Selected	Functional	Intersects With	5	Pre/Post Transmission Handling	CRY-01.3	Cryptographic mechanisms exist to ensure the confidentiality and integrity of information during preparation for transmission and during reception.	SC-8(2)	SC-8(2)	SC-8(2)	SC-8(2)	SC-08(02)	SC-08(02)	SC-08(02)	SC-08(02)	SC-8(2)	SC-8(2)	SC-8(2)	SC-8(2)	SC-8(2)					
SC	SC-08(02)	SC-8(2)	Transmission Confidentiality and Integrity | Pre- and Post-transmission Handling	Maintain the [Selection (one or more): confidentiality; integrity] of information during preparation for transmission and during reception.	SC-8(2)	Not Selected	Functional	Intersects With	5	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	SC-8(2)	SC-8(2)	SC-8(2)	SC-8(2)	SC-08(02)	SC-08(02)	SC-08(02)	SC-08(02)	SC-8(2)	SC-8(2)	SC-8(2)	SC-8(2)	SC-8(2)					
SC	SC-08(02)	SC-8(2)	Transmission Confidentiality and Integrity | Pre- and Post-transmission Handling	Maintain the [Selection (one or more): confidentiality; integrity] of information during preparation for transmission and during reception.	SC-8(2)	Not Selected	Functional	Intersects With	5	Media Use	DCH-10	Mechanisms exist to restrict the use of types of digital media on systems or system components.	SC-8(2)	SC-8(2)	SC-8(2)	SC-8(2)	SC-08(02)	SC-08(02)	SC-08(02)	SC-08(02)	SC-8(2)	SC-8(2)	SC-8(2)	SC-8(2)	SC-8(2)					
SC	SC-08(03)	SC-8(3)	Transmission Confidentiality and Integrity | Cryptographic Protection for Message Externals	Implement cryptographic mechanisms to protect message externals unless otherwise protected by [Assignment: organization-defined alternative physical controls].	SC-8(3)	Not Selected	Functional	Equal	10	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.																		
SC	SC-08(04)	SC-8(4)	Transmission Confidentiality and Integrity | Conceal or Randomize Communications	Implement cryptographic mechanisms to conceal or randomize communication patterns unless otherwise protected by [Assignment: organization-defined alternative physical controls].	SC-8(4)	Not Selected	Functional	Equal	10	Conceal / Randomize Communications	CRY-01.4	Cryptographic mechanisms exist to conceal or randomize communication patterns.																		
SC	SC-08(05)	SC-8(5)	Transmission Confidentiality and Integrity | Protected Distribution System	Implement [Assignment: organization-defined protected distribution system] to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.	SC-8(5)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SC	SC-09	SC-9	Withdrawn	Withdrawn	SC-9	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
SC	SC-10	SC-10	Network Disconnect	Terminate the network connection associated with a communications session at the end of the session or after [Assignment: organization-defined time period] of inactivity.	SC-10	Moderate	Functional	Equal	10	Network Connection Termination	NET-07	Mechanisms exist to terminate network connections at the end of a session or after an organization-defined time period of inactivity.		SC-10	SC-10			SC-10	SC-10							SC-10	SC-10		SC-10
SC	SC-11	SC-11	Trusted Path	Provide a [Selection (one): physically; logically] isolated trusted communications path for communications between the [Assignment: organization-defined security functions] and the user.	SC-11	Not Selected	Functional	Equal	10	Trusted Path	END-09	Mechanisms exist to establish a trusted communications path between the user and the security functions of the operating system.																		
SC	SC-11(01)	SC-11(1)	Trusted Path | Irrefutable Communications Path	Provide a trusted communications path that is irrefutably distinguishable from other communications paths for communications between the [Assignment: organization-defined security functions] and the user in accordance with the following key management requirements: [Assignment: organization-defined requirements].	SC-11(1)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SC	SC-12	SC-12	Cryptographic Key Establishment and Management	Establish and manage cryptographic keys for [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].	SC-12	Low	Functional	Intersects With	5	Public Key Infrastructure (PKI)	CRY-08	Mechanisms exist to securely implement an internal Public Key Infrastructure (PKI) infrastructure or obtain PKI services from a reputable PKI service provider.	SC-12	SC-12	SC-12		SC-12	SC-12	SC-12	SC-12					SC-12	SC-12	SC-12		SC-12
SC	SC-12(01)	SC-12(1)	Cryptographic Key Establishment and Management | Availability	Maintain availability of information in the event of the loss of cryptographic keys by users.	SC-12(1)	High	Functional	Equal	10	Cryptographic Key Loss or Change	CRY-09.3	Mechanisms exist to facilitate the availability of information in the event of the loss of cryptographic keys by individual users.			SC-12(01)				SC-12(01)										SC-12(01)
SC	SC-12(02)	SC-12(2)	Cryptographic Key Establishment and Management | Symmetric Keys	Produce, control, and distribute symmetric cryptographic keys using [Selection (one): NIST FIPS-validated; NSA-approved] key management technology and processes.	SC-12(2)	Not Selected	Functional	Equal	10	Symmetric Keys	CRY-09.1	Mechanisms exist to facilitate the production and management of symmetric cryptographic keys using Federal Information Processing Standards (FIPS)-compliant key management technology and processes.																SC-12(02)		SC-12(02)
SC	SC-12(03)	SC-12(3)	Cryptographic Key Establishment and Management | Asymmetric Keys	Produce, control, and distribute asymmetric cryptographic keys using [Selection (one): NSA-approved key management technology and processes; prequalified issuer; DoD-approved or DoD-issued Medium Assurance PKI certificates; DoD-approved or DoD-issued Medium Hardware Assurance PKI certificates; certificates issued in accordance with organization-defined requirements].	SC-12(3)	Not Selected	Functional	Equal	10	Asymmetric Keys	CRY-09.2	Mechanisms exist to facilitate the production and management of asymmetric cryptographic keys using Federal Information Processing Standards (FIPS)-compliant key management technology and processes.																SC-12(03)		SC-12(03)
SC	SC-12(04)	SC-12(4)	Withdrawn	Withdrawn	SC-12(4)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
SC	SC-12(05)	SC-12(5)	Withdrawn	Withdrawn	SC-12(5)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
SC	SC-12(06)	SC-12(6)	Cryptographic Key Establishment and Management | Physical Control of Keys	Maintain physical control of cryptographic keys when stored information is encrypted by external service providers.	SC-12(6)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SC	SC-13	SC-13	Cryptographic Protection	Implement [Assignment: organization-defined types of cryptography required for each specified cryptographic use; Assignment: organization-defined types of cryptography required for each specified cryptographic use; Assignment: organization-defined types of cryptography required for each specified cryptographic use; Assignment: organization-defined cryptographic uses; and Assignment: organization-defined types of cryptography required for each specified cryptographic use].	SC-13	Low	Functional	Intersects With	5	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	SC-13	SC-13	SC-13	SC-13	SC-13	SC-13	SC-13	SC-13	SC-13	SC-13	SC-13	SC-13	SC-13	SC-13	SC-13	SC-13	SC-13
SC	SC-13	SC-13	Cryptographic Protection	Implement [Assignment: organization-defined types of cryptography required for each specified cryptographic use; Assignment: organization-defined types of cryptography required for each specified cryptographic use; Assignment: organization-defined types of cryptography required for each specified cryptographic use; Assignment: organization-defined cryptographic uses; and Assignment: organization-defined types of cryptography required for each specified cryptographic use].	SC-13	Low	Functional	Intersects With	5	Export-Controlled Cryptography	CRY-01.2	Mechanisms exist to address the exporting of cryptographic technologies in compliance with relevant statutory and regulatory requirements.	SC-13	SC-13	SC-13	SC-13	SC-13	SC-13	SC-13	SC-13	SC-13	SC-13	SC-13	SC-13	SC-13	SC-13	SC-13	SC-13	SC-13
SC	SC-13	SC-13	Cryptographic Protection	Implement [Assignment: organization-defined types of cryptography required for each specified cryptographic use; Assignment: organization-defined types of cryptography required for each specified cryptographic use; Assignment: organization-defined types of cryptography required for each specified cryptographic use; Assignment: organization-defined cryptographic uses; and Assignment: organization-defined types of cryptography required for each specified cryptographic use].	SC-13	Low	Functional	Intersects With	5	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	SC-13	SC-13	SC-13	SC-13	SC-13	SC-13	SC-13	SC-13	SC-13	SC-13	SC-13	SC-13	SC-13	SC-13	SC-13	SC-13	SC-13
SC	SC-13(01)	SC-13(1)	Withdrawn	Withdrawn	SC-13(1)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
SC	SC-13(02)	SC-13(2)	Withdrawn	Withdrawn	SC-13(2)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
SC	SC-13(03)	SC-13(3)	Withdrawn	Withdrawn	SC-13(3)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
SC	SC-13(04)	SC-13(4)	Withdrawn	Withdrawn	SC-13(4)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
SC	SC-14	SC-14	Withdrawn	Withdrawn	SC-14	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
SC	SC-15	SC-15	Collaborative Computing Devices and Applications	Prohibit [Assignment: organization-defined exceptions where remote activation is to be allowed]; and b. Provide an explicit indication of use to users physically present at the devices.	SC-15	Low	Functional	Intersects With	5	Collaborative Computing Devices	END-14	Mechanisms exist to unplug or prohibit the remote activation of collaborative computing devices with the following exceptions: (1) Networked whiteboards; (2) Video teleconferencing cameras; and (3) Teleconference microphones.	SC-15	SC-15	SC-15		SC-15	SC-15	SC-15	SC-15										SC-15
SC	SC-15(01)	SC-15(1)	Collaborative Computing Devices and Applications | Physical or Logical Disconnect	Provide [Selection (one or more): physical; logical] disconnect of collaborative computing devices in a manner that supports ease of use.	SC-15(1)	Not Selected	Functional	Intersects With	5	Collaborative Computing Devices	END-14	Mechanisms exist to unplug or prohibit the remote activation of collaborative computing devices with the following exceptions: (1) Networked whiteboards; (2) Video teleconferencing cameras; and (3) Teleconference microphones.																		
SC	SC-15(02)	SC-15(2)	Withdrawn	Withdrawn	SC-15(2)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
SC	SC-15(03)	SC-15(3)	Collaborative Computing Devices and Applications | Disabling and Removal in Secure Work Areas	Disable or remove collaborative computing devices and applications from [Assignment: organization-defined systems or system components] in [Assignment: organization-defined secure work areas].	SC-15(3)	Not Selected	Functional	Equal	10	Disabling / Removal In Secure Work Areas	END-14.1	Mechanisms exist to disable or remove collaborative computing devices from critical systems and secure work areas.																		
SC	SC-15(04)	SC-15(4)	Collaborative Computing Devices and Applications | Explicitly Indicate Current Participants	Provide an explicit indication of current participants in [Assignment: organization-defined online meetings and teleconferences].	SC-15(4)	Not Selected	Functional	Equal	10	Explicitly Indicate Current Participants	END-14.2	Automated mechanisms exist to provide an explicit indication of current participants in online meetings and teleconferences.																		
SC	SC-16	SC-16	Transmission of Security and Privacy Attributes	Associate [Assignment: organization-defined security and privacy attributes] with information exchanged between [Assignment: organization-defined systems and system components].	SC-16	Not Selected	Functional	Intersects With	5	Transmission of Cybersecurity & Data Protection Attributes	CRY-10	Mechanisms exist to associate Technology Assets, Applications and/or Services (TAAS) security attributes with information exchanged between TAAS.																		
SC	SC-16(01)	SC-16(1)	Transmission of Security and Privacy Attributes | Integrity Verification	Verify the integrity of transmitted security and privacy attributes.	SC-16(1)	Not Selected	Functional	Intersects With	5	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	SC-16(1)	SC-16(1)	SC-16(1)	SC-16(1)	SC-16(01)	SC-16(01)	SC-16(01)	SC-16(01)	SC-16(1)	SC-16(1)	SC-16(1)	SC-16(1)	SC-16(1)					
SC	SC-16(01)	SC-16(1)	Transmission of Security and Privacy Attributes | Integrity Verification	Verify the integrity of transmitted security and privacy attributes.	SC-16(1)	Not Selected	Functional	Intersects With	5	Transmission of Cybersecurity & Data Protection Attributes	CRY-10	Mechanisms exist to associate Technology Assets, Applications and/or Services (TAAS) security attributes with information exchanged between TAAS.	SC-16(1)	SC-16(1)	SC-16(1)	SC-16(1)	SC-16(01)	SC-16(01)	SC-16(01)	SC-16(01)	SC-16(1)	SC-16(1)	SC-16(1)	SC-16(1)	SC-16(1)					
SC	SC-16(02)	SC-16(2)	Transmission of Security and Privacy Attributes | Anti-spoofing Mechanisms	Implement anti-spoofing mechanisms to prevent adversaries from falsifying the security attributes indicating the successful application of the security mechanisms bound to those attributes.	SC-16(2)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SC	SC-16(03)	SC-16(3)	Transmission of Security and Privacy Attributes | Cryptographic Binding	Implement the following mechanisms or techniques to bind security and privacy attributes to transmitted data: [Assignment: organization-defined mechanisms or techniques].	SC-16(3)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SC	SC-17	SC-17	Public Key Infrastructure Certificates	Issue public key certificates for [Assignment: organization-defined key certificates from an approved service provider; Assignment: organization-defined key certificates from an approved service provider; and Assignment: organization-defined key certificates from an approved service provider].	SC-17	Moderate	Functional	Intersects With	5	Public Key Infrastructure (PKI)	CRY-08	Mechanisms exist to securely implement an internal Public Key Infrastructure (PKI) infrastructure or obtain PKI services from a reputable PKI service provider.		SC-17	SC-17			SC-17	SC-17							SC-17	SC-17		SC-17
SC	SC-18	SC-18	Mobile Code	Define acceptable and unacceptable mobile code technologies; and b. Authorize, monitor, and control the use of mobile code within the system.	SC-18	Moderate	Functional	Intersects With	5	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-dependent applications.		SC-18	SC-18				SC-18							SC-18		SC-18	SC-18
SC	SC-18(01)	SC-18(1)	Mobile Code | Identify Unacceptable Code and Take Corrective Actions	Identify [Assignment: organization-defined unacceptable mobile code]; and take [Assignment: organization-defined corrective actions].	SC-18(1)	Not Selected	Functional	Intersects With	5	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	SC-18(1)	SC-18(1)	SC-18(1)	SC-18(1)	SC-18(01)	SC-18(01)	SC-18(01)	SC-18(01)	SC-18(1)	SC-18(1)	SC-18(1)	SC-18(1)	SC-18(1)					
SC	SC-18(01)	SC-18(1)	Mobile Code | Identify Unacceptable Code and Take Corrective Actions	Identify [Assignment: organization-defined unacceptable mobile code]; and take [Assignment: organization-defined corrective actions].	SC-18(1)	Not Selected	Functional	Intersects With	5	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-dependent applications.	SC-18(1)	SC-18(1)	SC-18(1)	SC-18(1)	SC-18(01)	SC-18(01)	SC-18(01)	SC-18(01)	SC-18(1)	SC-18(1)	SC-18(1)	SC-18(1)	SC-18(1)					
SC	SC-18(01)	SC-18(1)	Mobile Code | Identify Unacceptable Code and Take Corrective Actions	Identify [Assignment: organization-defined unacceptable mobile code]; and take [Assignment: organization-defined corrective actions].	SC-18(1)	Not Selected	Functional	Intersects With	5	Continuous Vulnerability Remediation Activities	VPM-04	Mechanisms exist to address new threats and vulnerabilities on an ongoing basis and ensure assets are protected against known attacks.	SC-18(1)	SC-18(1)	SC-18(1)	SC-18(1)	SC-18(01)	SC-18(01)	SC-18(01)	SC-18(01)	SC-18(1)	SC-18(1)	SC-18(1)	SC-18(1)	SC-18(1)					
SC	SC-18(02)	SC-18(2)	Mobile Code | Acquisition, Development, and Use	Determine the use of mobile code to be deployed in the system meets [Assignment: organization-defined requirements].	SC-18(2)	Not Selected	Functional	Intersects With	5	Software Licensing Restrictions	AST-02.7	Mechanisms exist to protect Intellectual Property (IP) rights with software licensing restrictions.	SC-18(2)	SC-18(2)	SC-18(2)	SC-18(2)	SC-18(02)	SC-18(02)	SC-18(02)	SC-18(02)	SC-18(2)	SC-18(2)	SC-18(2)	SC-18(2)	SC-18(2)					
SC	SC-18(02)	SC-18(2)	Mobile Code | Acquisition, Development, and Use	Determine the use of mobile code to be deployed in the system meets [Assignment: organization-defined requirements].	SC-18(2)	Not Selected	Functional	Intersects With	5	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-dependent applications.	SC-18(2)	SC-18(2)	SC-18(2)	SC-18(2)	SC-18(02)	SC-18(02)	SC-18(02)	SC-18(02)	SC-18(2)	SC-18(2

Family	Sorting Control #	Focal Document Element	Focal Document Element Name	Focal Document Element Description	NIST SP 800-53 R5.2	Security Control Baseline	Set Theory Relationship Mapping (STRM) Rationale	Set Theory Relationship Mapping (STRM) Relationship	Set Theory Relationship Mapping (STRM) Strength of Relationship	Reference Document Element	Reference Document Element Name	Reference Document Element Description	NIST SP 800-53 R5.2 Baselines Low	NIST SP 800-53 R5.2 Baselines Mod	NIST SP 800-53 R5.2 Baselines High	NIST SP 800-53 R5.2 Baselines Privacy	FedRAMP R5 Low	FedRAMP R5 Mod	FedRAMP R5 High	FedRAMP R5 LI-SaaS	NIST SP 800-161 R1 C-SCRM Baseline	NIST SP 800-161 R1 Low Impact Level Down	NIST SP 800-161 R1 Level 1	NIST SP 800-161 R1 Level 2	NIST SP 800-161 R1 Level 3	GovRAMP Low	GovRAMP Low+	GovRAMP Moderate	GovRAMP Core	GovRAMP High (FedRAMP Hi)
SC	SC-28(01)	SC-28(1)	Protection of Information at Rest | Cryptographic Protection	Protection of the following information at rest on [Assignment: organization-defined system components or media]: [Selection (one): confidentiality; integrity] using [Assignment: organization-defined cryptographic mechanisms]	SC-28(1)	Moderate	Functional	Intersects With	5	Cryptographic Protection	BCD-11.4	Cryptographic mechanisms exist to prevent the unauthorized disclosure and/or modification of backup information.	SC-28(1)	SC-28(1)	SC-28(1)	SC-28(1)	SC-28(01)	SC-28(01)	SC-28(01)	SC-28(01)	SC-28(1)	SC-28(1)	SC-28(1)	SC-28(1)	SC-28(1)			SC-28(01)		SC-28(01)
SC	SC-28(01)	SC-28(1)	Protection of Information at Rest | Cryptographic Protection	Protection of the following information at rest on [Assignment: organization-defined system components or media]: [Selection (one): confidentiality; integrity] using [Assignment: organization-defined cryptographic mechanisms]	SC-28(1)	Moderate	Functional	Intersects With	5	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	SC-28(1)	SC-28(1)	SC-28(1)	SC-28(1)	SC-28(01)	SC-28(01)	SC-28(01)	SC-28(01)	SC-28(1)	SC-28(1)	SC-28(1)	SC-28(1)	SC-28(1)			SC-28(01)		SC-28(01)
SC	SC-28(01)	SC-28(1)	Protection of Information at Rest | Cryptographic Protection	Protection of the following information at rest on [Assignment: organization-defined system components or media]: [Selection (one): confidentiality; integrity] using [Assignment: organization-defined cryptographic mechanisms]	SC-28(1)	Moderate	Functional	Intersects With	5	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	SC-28(1)	SC-28(1)	SC-28(1)	SC-28(1)	SC-28(01)	SC-28(01)	SC-28(01)	SC-28(01)	SC-28(1)	SC-28(1)	SC-28(1)	SC-28(1)	SC-28(1)			SC-28(01)		SC-28(01)
SC	SC-28(01)	SC-28(1)	Protection of Information at Rest | Cryptographic Protection	Protection of the following information at rest on [Assignment: organization-defined system components or media]: [Selection (one): confidentiality; integrity] using [Assignment: organization-defined cryptographic mechanisms]	SC-28(1)	Moderate	Functional	Intersects With	5	Encrypting Data In Storage Media	DCH-07.2	Cryptographic mechanisms exist to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.	SC-28(1)	SC-28(1)	SC-28(1)	SC-28(1)	SC-28(01)	SC-28(01)	SC-28(01)	SC-28(01)	SC-28(1)	SC-28(1)	SC-28(1)	SC-28(1)	SC-28(1)			SC-28(01)		SC-28(01)
SC	SC-28(02)	SC-28(2)	Protection of Information at Rest | Offline Storage	Protection of the following information at rest on [Assignment: organization-defined offline storage]: [Assignment: organization-defined controls]	SC-28(2)	Not Selected	Functional	Intersects With	5	Offline Storage	CRY-05.2	Mechanisms exist to remove unused data from online storage and archive it off-line in a secure location until it can be disposed of according to data retention requirements.	SC-28(2)	SC-28(2)	SC-28(2)	SC-28(2)	SC-28(02)	SC-28(02)	SC-28(02)	SC-28(02)	SC-28(2)	SC-28(2)	SC-28(2)	SC-28(2)	SC-28(2)					
SC	SC-28(02)	SC-28(2)	Protection of Information at Rest | Offline Storage	Protection of the following information at rest on [Assignment: organization-defined offline storage]: [Assignment: organization-defined controls]	SC-28(2)	Not Selected	Functional	Intersects With	5	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	SC-28(2)	SC-28(2)	SC-28(2)	SC-28(2)	SC-28(02)	SC-28(02)	SC-28(02)	SC-28(02)	SC-28(2)	SC-28(2)	SC-28(2)	SC-28(2)	SC-28(2)					
SC	SC-28(03)	SC-28(3)	Protection of Information at Rest | Cryptographic Keys	Protection of [Assignment: organization-defined information] at rest using [Selection (one): [Assignment: organization-defined cryptographic keys stored in [Assignment: organization-defined hardware-protected key store]]; [Assignment: organization-defined cryptographic keys stored in a key management technology and service]]	SC-28(3)	Not Selected	Functional	Equal	10	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.																	
SC	SC-29	SC-29	Heterogeneity	Employ a diverse set of information technologies for the following system components in the implementation of the system: [Assignment: organization-defined system components]	SC-29	Not Selected	Functional	Equal	10	Heterogeneity	SEA-13	Mechanisms exist to utilize a diverse set of technologies for system components to reduce the impact of technical vulnerabilities from the same Original Equipment Manufacturer (OEM).											SC-29	SC-29					
SC	SC-29(01)	SC-29(1)	Heterogeneity | Virtualization Techniques	Employ virtualization techniques to support the deployment of a diversity of operating systems and applications that are changed [Assignment: organization-defined frequency] [Assignment: organization-defined events] unless these techniques are impractical or unsupported in the following systems: [Assignment: organization-defined systems]	SC-29(1)	Not Selected	Functional	Equal	10	Virtualization Techniques	SEA-13.1	Mechanisms exist to utilize virtualization techniques to support the employment of a diversity of operating systems and applications.																	
SC	SC-30	SC-30	Concealment and Misdirection	Employ [Assignment: organization-defined concealment and misdirection techniques] for [Assignment: organization-defined systems] at [Assignment: organization-defined time periods] to confuse and mislead adversaries	SC-30	Not Selected	Functional	Intersects With	5	Concealment & Misdirection	SEA-14	Mechanisms exist to utilize concealment and misdirection techniques for Technology Assets, Applications and/or Services (TAAS) to confuse and mislead adversaries.											SC-30	SC-30					
SC	SC-30(01)	SC-30(1)		Withdrawn	SC-30(1)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																	
SC	SC-30(02)	SC-30(2)	Concealment and Misdirection | Randomness	Employ [Assignment: organization-defined techniques] to introduce randomness into organizational operations and assets	SC-30(2)	Not Selected	Functional	Equal	10	Randomness	SEA-14.1	Automated mechanisms exist to introduce randomness into organizational operations and assets.											SC-30(2)	SC-30(2)					
SC	SC-30(03)	SC-30(3)	Concealment and Misdirection | Change Processing and Storage Locations	Change the processing and storage [Selection (one): [Assignment: organization-defined time frequency]; at [Assignment: organization-defined time intervals]; at random time intervals]	SC-30(3)	Not Selected	Functional	Equal	10	Change Processing & Storage Locations	SEA-14.2	Automated mechanisms exist to change the location of processing and/or storage at random time intervals.											SC-30(3)	SC-30(3)					
SC	SC-30(04)	SC-30(4)	Concealment and Misdirection | Misleading Information	Employ realistic, but misleading information in [Assignment: organization-defined system components] with respect to [Assignment: organization-defined techniques]	SC-30(4)	Not Selected	Functional	Intersects With	5	Concealment & Misdirection	SEA-14	Mechanisms exist to utilize concealment and misdirection techniques for Technology Assets, Applications and/or Services (TAAS) to confuse and mislead adversaries.											SC-30(4)	SC-30(4)					
SC	SC-30(05)	SC-30(5)	Concealment and Misdirection | Concealment of System Components	Employ the following techniques to hide or conceal [Assignment: organization-defined system components]: [Assignment: organization-defined techniques]	SC-30(5)	Not Selected	Functional	Intersects With	5	Concealment & Misdirection	SEA-14	Mechanisms exist to utilize concealment and misdirection techniques for Technology Assets, Applications and/or Services (TAAS) to confuse and mislead adversaries.											SC-30(5)	SC-30(5)					
SC	SC-31	SC-31	Covert Channel Analysis	Perform a covert channel analysis to identify those potential avenues for covert [Selection (one or more): storage; timing] channels to be exploited	SC-31	Not Selected	Functional	Equal	10	Covert Channel Analysis	MON-15	Mechanisms exist to conduct covert channel analysis to identify aspects of communications that are potential avenues for covert channels.																	
SC	SC-31(01)	SC-31(1)	Covert Channel Analysis | Test Covert Channels for Exploitability	Test a subset of the identified covert channels to determine the channels that are exploitable.	SC-31(1)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
SC	SC-31(02)	SC-31(2)	Covert Channel Analysis | Maximum Bandwidth	Reduce the maximum bandwidth for identified covert [Selection (one or more): storage; timing] channels to [Assignment: organization-defined values]	SC-31(2)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
SC	SC-31(03)	SC-31(3)	Covert Channel Analysis | Measure Bandwidth in Operational Environments	Measure the bandwidth of [Assignment: organization-defined subset of identified covert channels] in the operational environments of the system	SC-31(3)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
SC	SC-32	SC-32	System Partitioning	Partition the system into [Assignment: organization-defined system components] with [Selection (one): physical; logical] domains or environments based on [Assignment: organization-defined circumstances for physical or logical separation of components]	SC-32	Not Selected	Functional	Equal	10	System Partitioning	SEA-03.1	Mechanisms exist to partition systems so that partitions reside in separate physical domains or environments.																	
SC	SC-32(01)	SC-32(1)	System Partitioning | Separate Physical Domains for Privileged Functions	Partition privileged functions into separate physical domains.	SC-32(1)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
SC	SC-33	SC-33		Withdrawn	SC-33	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																	
SC	SC-34	SC-34	Non-modifiable Executable Programs	For [Assignment: organization-defined system components] that load and execute the operating environment from hardware-enforced, read-only media; and [Assignment: organization-defined system components] that load and execute [Assignment: organization-defined applications] from hardware-enforced, read-only media	SC-34	Not Selected	Functional	Equal	10	Non-Modifiable Executable Programs	SEA-16	Mechanisms exist to utilize non-modifiable executable programs that load and execute the operating environment and applications from hardware-enforced, read-only media.																	
SC	SC-34(01)	SC-34(1)	Non-modifiable Executable Programs | No Writable Storage	Employ [Assignment: organization-defined system components] with no writable storage that is persistent across restart or power on/off	SC-34(1)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
SC	SC-34(02)	SC-34(2)	Non-modifiable Executable Programs | Integrity Protection on Read-only Media	For [Assignment: organization-defined system components] that load and execute [Assignment: organization-defined applications] from hardware-enforced, read-only media, protect the integrity of information prior to storage on read-only media and control the media after such information is written to the media	SC-34(2)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
SC	SC-34(03)	SC-34(3)		Withdrawn	SC-34(3)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																	
SC	SC-35	SC-35	External Malicious Code Identification	Include components [Assignment: organization-defined externally-provided components] in [Assignment: organization-defined frequency] scans for malicious code	SC-35	Not Selected	Functional	Equal	10	Honeyclients	SEA-12	Mechanisms exist to utilize honeyclients that proactively seek to identify malicious websites and/or web-based malicious code.																	
SC	SC-36	SC-36	Distributed Processing and Storage	Distribute the following processing and storage components across multiple [Selection (one): physical locations; logical domains]: [Assignment: organization-defined processing and storage components]; and [Assignment: organization-defined time intervals] or [Selection (one): event-driven; organization-defined events]	SC-36	Not Selected	Functional	Equal	10	Distributed Processing & Storage	SEA-15	Mechanisms exist to distribute processing and storage across multiple physical locations.											SC-36	SC-36					
SC	SC-36(01)	SC-36(1)	Distributed Processing and Storage | Polling Techniques	Employ polling techniques to identify potential faults, errors, or compromises to the following distributed processing and storage components: [Assignment: organization-defined distributed processing and storage components]; and [Assignment: organization-defined time intervals] or [Selection (one): event-driven; organization-defined events]	SC-36(1)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
SC	SC-36(02)	SC-36(2)	Distributed Processing and Storage | Synchronization	Synchronize the following duplicate systems or system components: [Assignment: organization-defined duplicate systems or system components]	SC-36(2)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
SC	SC-37	SC-37	Out-of-band Channels	Employ [Assignment: organization-defined out-of-band channels] for the physical delivery or electronic transmission of [Assignment: organization-defined information, system components, or devices] to [Assignment: organization-defined individuals or systems]	SC-37	Not Selected	Functional	Intersects With	5	Out-of-Band Channels	NET-11	Mechanisms exist to utilize out-of-band channels for the electronic transmission of information and/or the physical shipment of system components or devices to authorized individuals or systems.																	
SC	SC-37(01)	SC-37(1)	Out-of-band Channels | Ensure Delivery and Transmission	Employ [Assignment: organization-defined controls] to ensure that only [Assignment: organization-defined individuals or systems] receive the following information, system components, or devices: [Assignment: organization-defined information, system components, or devices]	SC-37(1)	Not Selected	Functional	Intersects With	5	Out-of-Band Channels	NET-11	Mechanisms exist to utilize out-of-band channels for the electronic transmission of information and/or the physical shipment of system components or devices to authorized individuals or systems.											SC-37(1)	SC-37(1)					
SC	SC-38	SC-38	Operations Security	Implement the following operations security controls to protect key organizational information throughout the system development life cycle: [Assignment: organization-defined information]	SC-38	Not Selected	Functional	Intersects With	5	Security Operations Center (SOC)	OPS-04	Mechanisms exist to establish and maintain a Security Operations Center (SOC) that facilitates a 24x7 response capability.	SC-38	SC-38	SC-38	SC-38	SC-38	SC-38	SC-38	SC-38	SC-38	SC-38	SC-38	SC-38	SC-38					
SC	SC-38	SC-38	Operations Security	Implement the following operations security controls to protect key organizational information throughout the system development life cycle: [Assignment: organization-defined information]	SC-38	Not Selected	Functional	Intersects With	5	Operations Security	OPS-01	Mechanisms exist to facilitate the implementation of operational security controls.	SC-38	SC-38	SC-38	SC-38	SC-38	SC-38	SC-38	SC-38	SC-38	SC-38	SC-38	SC-38	SC-38					
SC	SC-39	SC-39	Process Isolation	Maintain a separate execution domain for each executing system process	SC-39	Low	Functional	Equal	10	Process Isolation	SEA-04	Mechanisms exist to implement a separate execution domain for each executing process.	SC-39	SC-39	SC-39		SC-39	SC-39	SC-39	SC-39						SC-39	SC-39	SC-39		SC-39
SC	SC-39(01)	SC-39(1)	Process Isolation | Hardware Separation	Implement hardware separation mechanisms to facilitate process isolation	SC-39(1)	Not Selected	Functional	Equal	10	Hardware Separation	SEA-04.2	Mechanisms exist to implement underlying hardware separation mechanisms to facilitate process separation.																	
SC	SC-39(02)	SC-39(2)	Process Isolation | Separate Execution Domain Per Thread	Maintain a separate execution domain for each thread in [Assignment: organization-defined multi-threaded processing]	SC-39(2)	Not Selected	Functional	Equal	10	Thread Separation	SEA-04.3	Mechanisms exist to maintain a separate execution domain for each thread in multi-threaded processing.																	
SC	SC-40	SC-40	Wireless Link Protection	Protect external and internal [Assignment: organization-defined wireless links] from the following signal parameter attacks: [Assignment: organization-defined types of signal parameter attacks or references to sources for such attacks]	SC-40	Not Selected	Functional	Intersects With	5	Wireless Link Protection	NET-12.1	Mechanisms exist to protect wireless and external wireless links from signal parameter attacks through monitoring for unauthorized wireless connections, including scanning for unauthorized wireless access points and taking appropriate action, if an unauthorized connection is discovered.	SC-40	SC-40	SC-40	SC-40	SC-40	SC-40	SC-40	SC-40	SC-40	SC-40	SC-40	SC-40	SC-40					
SC	SC-40	SC-40	Wireless Link Protection	Protect external and internal [Assignment: organization-defined wireless links] from the following signal parameter attacks: [Assignment: organization-defined types of signal parameter attacks or references to sources for such attacks]	SC-40	Not Selected	Functional	Intersects With	5	Wireless Access Authentication & Encryption	CRY-07	Mechanisms exist to protect wireless access via secure authentication and encryption.	SC-40	SC-40	SC-40	SC-40	SC-40	SC-40	SC-40	SC-40	SC-40	SC-40	SC-40	SC-40	SC-40					
SC	SC-40(01)	SC-40(1)	Wireless Link Protection | Electromagnetic Interference	Implement cryptographic mechanisms that achieve [Assignment: organization-defined level of protection] against the effects of intentional electromagnetic interference	SC-40(1)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
SC	SC-40(02)	SC-40(2)	Wireless Link Protection | Reduce Detection Potential	Implement cryptographic mechanisms that reduce the detection potential of wireless links to [Assignment: organization-defined level of reduction]	SC-40(2)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
SC	SC-40(03)	SC-40(3)	Wireless Link Protection | Imitative or Manipulative Communications Deception	Implement cryptographic mechanisms to identify and reject wireless transmissions that are deliberate attempts to achieve imitative or manipulative communications deception based on signal parameters	SC-40(3)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
SC	SC-40(04)	SC-40(4)	Wireless Link Protection | Signal Parameter Identification	Implement cryptographic mechanisms to prevent the identification of [Assignment: organization-defined wireless transmitters] by using the transmitter signal parameters	SC-40(4)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
SC	SC-41	SC-41	Port and I/O Device Access	[Selection (one): physically; logically] disable or remove [Assignment: organization-defined connection ports or input/output devices] on the following systems or system components: [Assignment: organization-defined systems or system components]	SC-41	Not Selected	Functional	Equal	10	Port & Input / Output (I/O) Device Access	END-12	Mechanisms exist to physically disable or remove unnecessary connection ports or input/output devices from sensitive systems.																	
SC	SC-42	SC-42	Sensor Capability and Data	(a) Prohibit the remote activation of environmental sensing capabilities with the following exceptions: [Assignment: organization-defined exceptions where remote activation of sensors is allowed]; and (b) Provide an explicit indication of sensor use to [Assignment: organization-defined group of users]	SC-42	Not Selected	Functional	Equal	10	Sensor Capability	END-13	(1) Prohibit the remote activation of sensing capabilities; and (2) Provide an explicit indication of sensor use.																	
SC	SC-42(01)	SC-42(1)	Sensor Capability and Data | Reporting to Authorized Individuals or Roles	Verify that the following sensors in the following systems are configured so that data collected by the [Assignment: organization-defined sensors] is only reported to authorized individuals or roles: [Assignment: organization-defined sensors]; [Assignment: organization-defined systems]	SC-42(1)	Not Selected	Functional	Equal	10	Sensor Delivery Verification	END-13.4	Mechanisms exist to verify embedded technology sensors are configured so that data collected by the sensor(s) is only reported to authorized individuals or roles.																	
SC	SC-42(02)	SC-42(2)	Sensor Capability and Data | Authorized Use	Employ the following measures so that data or information collected by [Assignment: organization-defined sensors] is only used for authorized purposes: [Assignment: organization-defined measures]	SC-42(2)	Not Selected	Functional	Equal	10	Authorized Use	END-13.1	Mechanisms exist to utilize organization-defined measures so that data or information collected by sensors is only used for authorized purposes.																	
SC	SC-42(03)	SC-42(3)		Withdrawn	SC-42(3)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																	
SC	SC-42(04)	SC-42(4)	Sensor Capability and Data | Notice of Collection	Employ a mechanism that provides [Assignment: organization-defined individuals with reasonable notice] with respect to the collection of [Assignment: organization-defined sensory information]	SC-42(4)	Not Selected	Functional	Equal	10	Notice of Collection	END-13.2	Mechanisms exist to notify individuals that Personal Data (PD) is collected by sensors.																	
SC	SC-42(05)	SC-42(5)	Sensor Capability and Data | Collection Minimization	Employ [Assignment: organization-defined sensors] that are configured to minimize the collection of information about [Assignment: organization-defined individuals]	SC-42(5)	Not Selected	Functional	Equal	10	Collection Minimization	END-13.3	Mechanisms exist to utilize sensors that are configured to minimize the collection of information about individuals.																	
SC	SC-43	SC-43	Usage Restrictions	(a) Establish usage restrictions and implementation guidance for the following system components: [Assignment: organization-defined system components]; and (b) Authorize, monitor, and control the use of such components within the system.	SC-43	Not Selected	Functional	Equal	10	Usage Parameters	AST-14	Mechanisms exist to monitor, enforce usage parameters that limit the potential damage caused from the unauthorized or unintentional alteration of system parameters.																	
SC	SC-44	SC-44	Detonation Chambers	Employ a detonation chamber capability within [Assignment: organization-defined system, system component, or location]	SC-44	Not Selected	Functional	Equal	10	Detonation Chambers (Sandboxes)	IRO-15	Mechanisms exist to utilize a detonation chamber capability to detect and/or block potentially-malicious files and email attachments.																	
SC	SC-45	SC-45	System Time Synchronization	Synchronize system clocks within and between systems and system components.	SC-45	Not Selected	Functional	Intersects With	5	Synchronization With Authoritative Time Source	MON-07.1	Mechanisms exist to synchronize internal system clocks with an authoritative time source.						SC-45	SC-45										
SC	SC-45(01)	SC-45(1)	System Time Synchronization | Synchronization with Authoritative Time Source	(a) Compare the internal system clocks [Assignment: organization-defined frequency] with [Assignment: organization-defined authoritative time source]; and (b) Synchronize the internal system clocks to the authoritative time source when the time difference is greater than [Assignment: organization-defined time period]	SC-45(1)	Not Selected	Functional	Equal	10	Synchronization With Authoritative Time Source	MON-07.1	Mechanisms exist to synchronize internal system clocks with an authoritative time source.						SC-45(01)	SC-45(01)										
SC	SC-45(02)	SC-45(2)	System Time Synchronization | Secondary Authoritative Time Source	(a) Identify secondary authoritative time sources that are in different [Assignment: organization-defined geographic regions] than primary authoritative time sources; and (b) Synchronize the internal system clocks to the secondary authoritative time source if the primary authoritative time source is unavailable	SC-45(2)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
SC	SC-46	SC-46	Cross Domain Policy Enforcement	Implement a policy enforcement mechanism [Selection (one): physically; logically] between the physical and/or network interfaces for the following communications paths: [Assignment: organization-defined communications paths] for system operations	SC-46	Not Selected	Functional	Equal	10	Cross Domain Solution (CDS)	NET-02.3	Mechanisms exist to implement a Cross Domain Solution (CDS) to mitigate the specific security risks of accessing or transferring information between security domains.																	
SC	SC-47	SC-47	Alternate Communications Channels	Establish [Assignment: organization-defined alternate communications paths] for system operations	SC-47	Not Selected	Functional	Equal	10	Alternate Communications Channels	BCD-10.4	Mechanisms exist to maintain command and control capabilities via alternate communications channels and designating alternative decision makers if primary decision makers are unavailable.									SC-47	SC-47	SC-47						
SC	SC-48	SC-48	Sensor Relocation	Employ sensors at the following external and internal [Assignment: organization-defined locations] under the following conditions or circumstances: [Assignment: organization-defined conditions or circumstances]; [Assignment: organization-defined frequency]	SC-48	Not Selected	Functional	Intersects With	5	Threat Hunting	THR-07	Mechanisms exist to perform cyber threat hunting that uses Indicators of Compromise (IoC) to detect, track and disrupt threats that evade existing security controls.	SC-48	SC-48	SC-48	SC-48	SC-48	SC-48	SC-48	SC-48	SC-48	SC-48	SC-48	SC-48	SC-48					
SC	SC-48	SC-48	Sensor Relocation	Employ sensors at the following external and internal [Assignment: organization-defined locations] under the following conditions or circumstances: [Assignment: organization-defined conditions or circumstances]; [Assignment: organization-defined frequency]	SC-48	Not Selected	Functional	Intersects With	5	Automated Tools for Real-Time Analysis	MON-01.2	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support near real-time analysis and incident escalation.	SC-48	SC-48	SC-48	SC-48	SC-48	SC-48	SC-48	SC-48	SC-48	SC-48	SC-48	SC-48	SC-48					
SC	SC-48(01)	SC-48(1)	Sensor Relocation | Dynamic Relocation of Sensors or Monitoring Capabilities	Relocate the following sensors and monitoring capabilities [Assignment: organization-defined locations] under the following conditions: [Assignment: organization-defined conditions]	SC-48(1)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
SC	SC-49	SC-49	Hardware-enforced Separation and Policy Enforcement	Implement hardware-enforced separation and policy enforcement mechanisms between [Assignment: organization-defined system components]	SC-49	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
SC	SC-50	SC-50	Software-enforced Separation and Policy Enforcement	Implement software-enforced separation and policy enforcement mechanisms between [Assignment: organization-defined system components]	SC-50	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
SC	SC-51	SC-51	Hardware-based Protection	(a) [Selection (one): Implement; Maintain] hardware-based controls that the system will employ when installing and booting firmware components to ensure the integrity of system firmware components; and (b) Monitor the integrity of the hardware-based controls [Assignment: organization-defined authorized	SC-51	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
SI	SI-01	SI-1	Policy and Procedures	Develop, document, and maintain a Cybersecurity & Data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their	GOV-03	Low	Functional	Intersects With	5	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their	SI-1	SI-1	SI-1	SI-1	SI-01	SI-01	SI-01	SI-01	SI-1	SI-1	SI-1	SI-1	SI-1	SI-01	SI-01	SI-01		SI-01
SI	SI-01	SI-1	Policy and Procedures	Develop, document, and maintain policy and procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls;	SI-1	Low	Functional	Subset Of	10	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity and data protection practices in the specification, design, development, implementation and modification of	SI-1	SI-1	SI-1	SI-1	SI-01	SI-01	SI-01	SI-01	SI-1	SI-1	SI-1	SI-1	SI-1	SI-01	SI-01	SI-01		SI-01
SI	SI-01	SI-1	Policy and Procedures	Develop, document, and maintain policy and procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls;	SI-1	Low	Functional	Intersects With	5	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	SI-1	SI-1	SI-1	SI-1	SI-01	SI-01	SI-01	SI-01	SI-1	SI-1	SI-1	SI-1	SI-1	SI-01	SI-01	SI-01		SI-01
SI	SI-02	SI-2	Flaw Remediation	Identify, report, and correct system flaws;	SI-2	Low	Functional	Intersects With	5	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	SI-2	SI-2	SI-2	SI-2	SI-02	SI-02	SI-02	SI-02	SI-2	SI-2	SI-2	SI-2	SI-2	SI-02	SI-02	SI-02	SI-02	SI-02
SI	SI-02	SI-2	Flaw Remediation	Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;	SI-2	Low	Functional	Intersects With	5	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	SI-2	SI-2	SI-2	SI-2	SI-02	SI-02	SI-02	SI-02	SI-2	SI-2	SI-2	SI-2	SI-2	SI-02	SI-02	SI-02	SI-02	SI-02
SI	SI-02	SI-2	Flaw Remediation	Install security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates; and	SI-2	Low	Functional	Intersects With	5	Automatic Antimalware Signature Updates	END-04.1	Automated mechanisms exist to update antimalware technologies, including signature definitions.	SI-2	SI-2	SI-2	SI-2	SI-02	SI-02	SI-02	SI-02	SI-2	SI-2	SI-2	SI-2	SI-2	SI-02	SI-02	SI-02	SI-02	SI-02
SI	SI-02	SI-2	Flaw Remediation	Incorporate flaw remediation into the organizational configuration management process.	SI-2	Low	Functional	Intersects With	5	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	SI-2	SI-2	SI-2	SI-2	SI-02	SI-02	SI-02	SI-02	SI-2	SI-2	SI-2	SI-2	SI-2	SI-02	SI-02	SI-02	SI-02	SI-02
SI	SI-02(01)	SI-2(1)		Withdrawn	SI-2(1)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																	
SI	SI-02(02)	SI-2(2)	Flaw Remediation | Automated Flaw Remediation Status	Determine if [Assignment: organization-defined installed software] is [Assignment: organization-defined software and firmware components] are current	SI-2(2)	Moderate	Functional	Intersects With	5	Automated Remediation Status	VPM-05.2	Automated mechanisms exist to determine the state of system components with regard to flaw remediation.		SI-2(2)	SI-2(2)			SI-02(02)	SI-02(02)								SI-02(02)	SI-02(02)	SI-02(02)	
SI	SI-02(03)	SI-2(3)	Flaw Remediation | Time to Remediate Flaws and Benchmarks for Corrective Actions	Measure the time between flaw identification and flaw remediation; and Establish the following benchmarks for taking corrective actions: [Assignment: organization-defined benchmarks]	SI-2(3)	Not Selected	Functional	Equal	10	Time To Remediate / Benchmarks For Corrective Action	VPM-05.3	Mechanisms exist to track the effectiveness of remediation operations through metrics reporting.						SI-02(03)	SI-02(03)								SI-02(03)		SI-02(03)	
SI	SI-02(04)	SI-2(4)	Flaw Remediation | Automated Patch Management Tools	Update the following system components using automated patch management tools consistent with the system's configuration management policy and procedures: [Assignment: organization-defined system components]	SI-2(4)	Not Selected	Functional	Intersects With	5	Automated Remediation Status	VPM-05.2	Automated mechanisms exist to determine the state of system components with regard to flaw remediation.	SI-2(4)	SI-2(4)	SI-2(4)	SI-2(4)	SI-02(04)	SI-02(04)	SI-02(04)	SI-02(04)	SI-2(4)	SI-2(4)	SI-2(4)	SI-2(4)	SI-2(4)					
SI	SI-02(04)	SI-2(4)	Flaw Remediation | Automated Patch Management Tools	Update the following system components using automated patch management tools consistent with the system's configuration management policy and procedures: [Assignment: organization-defined system components]	SI-2(4)	Not Selected	Funct

Family	Sorting Control #	Focal Document Element	Focal Document Element Name	Focal Document Element Description	NIST SP 800-53 R5.2	Security Control Baseline	Set Theory Relationship Mapping (STRM) Rationale	Set Theory Relationship Mapping (STRM) Relationship	Strength of Relationship	Reference Document Element	Reference Document Element Name	Reference Document Element Description	NIST SP 800-53 R5.2 Baselines Low	NIST SP 800-53 R5.2 Baselines Mod	NIST SP 800-53 R5.2 Baselines High	NIST SP 800-53 R5.2 Baselines Privacy	FedRAMP R5 Low	FedRAMP R5 Mod	FedRAMP R5 High	FedRAMP R5 LI-SaaS	NIST SP 800-161 R1 C-SCRM Baseline	NIST SP 800-161 R1 Cybersecurity Supply Chain Risk Management Overlay	NIST SP 800-161 R1 Level 1	NIST SP 800-161 R1 Level 2	NIST SP 800-161 R1 Level 3	GovRAMP Low	GovRAMP Low+	GovRAMP Moderate	GovRAMP Core	GovRAMP High (FedRAMP Rev. 5)
SI	SI-04	SI-4	System Monitoring	determined essential information: and2. At ad hoc locations within the system to track specific types of	SI-4	Low	Functional	Intersects With	5	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	SI-4	SI-4	SI-4	SI-4	SI-04	SI-04	SI-04	SI-04	SI-4	SI-4	SI-4	SI-4	SI-4	SI-04	SI-04	SI-04	SI-04	SI-04
SI	SI-04	SI-4	System Monitoring	determined essential information: and2. At ad hoc locations within the system to track specific types of	SI-4	Low	Functional	Intersects With	5	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM) or similar automated tool, to support the centralized collection of security-related event logs.	SI-4	SI-4	SI-4	SI-4	SI-04	SI-04	SI-04	SI-04	SI-4	SI-4	SI-4	SI-4	SI-4	SI-04	SI-04	SI-04	SI-04	SI-04
SI	SI-04	SI-4	System Monitoring	determined essential information: and2. At ad hoc locations within the system to track specific types of	SI-4	Low	Functional	Intersects With	5	Safeguarding Data Over Open Networks	NET-12	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.	SI-4	SI-4	SI-4	SI-4	SI-04	SI-04	SI-04	SI-04	SI-4	SI-4	SI-4	SI-4	SI-4	SI-04	SI-04	SI-04	SI-04	SI-04
SI	SI-04	SI-4	System Monitoring	determined essential information: and2. At ad hoc locations within the system to track specific types of	SI-4	Low	Functional	Intersects With	5	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	SI-4	SI-4	SI-4	SI-4	SI-04	SI-04	SI-04	SI-04	SI-4	SI-4	SI-4	SI-4	SI-4	SI-04	SI-04	SI-04	SI-04	SI-04
SI	SI-04(01)	SI-4(1)	System Monitoring | System-wide Intrusion Detection	Connect and configure individual intrusion detection	SI-4(1)	Not Selected	Functional	Equal	10	Intrusion Detection & Prevention Systems (IDS & IPS)	MON-01.1	Mechanisms exist to implement Intrusion Detection / Prevention Systems (IDS / IPS) technologies on critical systems, key network segments and network choke points.		SI-4(01)	SI-4(01)										SI-04(01)			SI-04(01)
SI	SI-04(02)	SI-4(2)	System Monitoring | Automated Tools and Mechanisms for Real-Time Analysis	tools and mechanisms to support	SI-4(2)	Moderate	Functional	Equal	10	Automated Tools for Real-Time Analysis	MON-01.2	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support near real-time analysis and incident escalation.		SI-4(2)	SI-4(2)			SI-04(02)	SI-04(02)								SI-04(02)			SI-04(02)
SI	SI-04(03)	SI-4(3)	System Monitoring | Automated Tool and Mechanism Integration		SI-4(3)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SI	SI-04(04)	SI-4(4)	System Monitoring | Inbound and Outbound Communications Traffic	communications traffic]; Monitor inbound and outbound	SI-4(4)	Moderate	Functional	Equal	10	Inbound & Outbound Communications Traffic	MON-01.3	Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.		SI-4(4)	SI-4(4)			SI-04(04)	SI-04(04)								SI-04(04)	SI-04(04)	SI-04(04)	SI-04(04)
SI	SI-04(05)	SI-4(5)	System Monitoring | System-generated Alerts	of compromise or potential compromise occur:	SI-4(5)	Moderate	Functional	Equal	10	System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data protection and supply chain activities to achieve integrated situational awareness.		SI-4(5)	SI-4(5)			SI-04(05)	SI-04(05)								SI-04(05)			SI-04(05)
SI	SI-04(06)	SI-4(6)		Withdrawn	SI-4(6)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
SI	SI-04(07)	SI-4(7)	System Monitoring | Automated Response to Suspicious Events	of suspicious events; and\b. Take the following actions upon detection: [Assignment: organization-	SI-4(7)	Not Selected	Functional	Intersects With	5	Automated Response to Suspicious Events	MON-01.11	Automated mechanisms exist to implement pre-determined corrective actions in response to detected events that have security incident implications.	SI-4(7)	SI-4(7)	SI-4(7)	SI-4(7)	SI-04(07)	SI-04(07)	SI-04(07)	SI-04(07)	SI-4(7)	SI-4(7)	SI-4(7)	SI-4(7)	SI-4(7)					
SI	SI-04(07)	SI-4(7)	System Monitoring | Automated Response to Suspicious Events	of detected suspicious events; and\b. Take the following actions upon detection: [Assignment: organization-	SI-4(7)	Not Selected	Functional	Intersects With	5	Automated Incident Handling Processes	IRO-02.1	Automated mechanisms exist to support the incident handling process.	SI-4(7)	SI-4(7)	SI-4(7)	SI-4(7)	SI-04(07)	SI-04(07)	SI-04(07)	SI-04(07)	SI-4(7)	SI-4(7)	SI-4(7)	SI-4(7)	SI-4(7)					
SI	SI-04(08)	SI-4(8)		Withdrawn	SI-4(8)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
SI	SI-04(09)	SI-4(9)	System Monitoring | Testing of Monitoring Tools and Mechanisms	Test intrusion-monitoring tools and mechanisms [Assignment: organization-defined frequency];	SI-4(9)	Not Selected	Functional	Intersects With	5	Incident Response Testing	IRO-06	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.																		
SI	SI-04(10)	SI-4(10)	System Monitoring | Visibility of Encrypted Communications	defined encrypted communications traffic] is visible to	SI-4(10)	High	Functional	Equal	10	Visibility of Encrypted Communications	NET-18.2	Mechanisms exist to configure the proxy to make encrypted communications traffic visible to monitoring tools and mechanisms.			SI-4(10)				SI-04(10)											
SI	SI-04(11)	SI-4(11)	System Monitoring | Analyze Communications Traffic Anomalies	interfaces to the system and selected [Assignment: organization-defined interior points within the system] to	SI-4(11)	Not Selected	Functional	Equal	10	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise							SI-04(11)										SI-04(11)
SI	SI-04(12)	SI-4(12)	System Monitoring | Automated Organization-generated Alerts	automated mechanisms] when the following indications	SI-4(12)	High	Functional	Intersects With	5	Automated Alerts	MON-01.12	Mechanisms exist to automatically alert incident response personnel to inappropriate or anomalous activities that have potential security incident implications.	SI-4(12)	SI-4(12)	SI-4(12)	SI-4(12)	SI-04(12)	SI-04(12)	SI-04(12)	SI-04(12)	SI-4(12)	SI-4(12)	SI-4(12)	SI-4(12)	SI-4(12)					
SI	SI-04(12)	SI-4(12)	System Monitoring | Automated Organization-generated Alerts	of inappropriate or unusual activities with security or	SI-4(12)	High	Functional	Intersects With	5	Real-Time Alerts of Event Logging Failure	MON-05.1	Mechanisms exist to provide 24x7x365 near real-time alerting capability when an event log processing failure occurs.	SI-4(12)	SI-4(12)	SI-4(12)	SI-4(12)	SI-04(12)	SI-04(12)	SI-04(12)	SI-04(12)	SI-4(12)	SI-4(12)	SI-4(12)	SI-4(12)	SI-4(12)					
SI	SI-04(13)	SI-4(13)	System Monitoring | Analyze Traffic and Event Patterns	the system:b. Develop profiles representing common	SI-4(13)	Not Selected	Functional	Equal	10	Alert Threshold Tuning	MON-01.13	Mechanisms exist to "tune" event monitoring technologies through analyzing communications traffic/event patterns and developing profiles representing common traffic patterns and/or events.																		
SI	SI-04(14)	SI-4(14)	System Monitoring | Wireless Intrusion Detection	rogue wireless devices and to detect attack attempts	SI-4(14)	High	Functional	Intersects With	5	Wireless Network Monitoring	MON-01.5	(1) Rogue wireless devices; and			SI-4(14)				SI-04(14)								SI-04(14)		SI-04(14)
SI	SI-04(14)	SI-4(14)	System Monitoring | Wireless Intrusion Detection	rogue wireless devices and to detect attack attempts	SI-4(14)	High	Functional	Intersects With	5	Prevention Systems (WIDS / WIPS)	NET-08.2	Mechanisms exist to utilize Wireless Intrusion Detection / Protection Systems (WIDS / WIPS) on wireless network segments.			SI-4(14)				SI-04(14)								SI-04(14)		SI-04(14)
SI	SI-04(15)	SI-4(15)	System Monitoring | Wireless to Wireline Communications	wireless communications traffic as the traffic passes	SI-4(15)	Not Selected	Functional	Intersects With	5	Wireless Network Monitoring	MON-01.5	(1) Rogue wireless devices; and							SI-04(15)										
SI	SI-04(15)	SI-4(15)	System Monitoring | Wireless to Wireline Communications	wireless communications traffic as the traffic passes	SI-4(15)	Not Selected	Functional	Intersects With	5	Prevention Systems (WIDS / WIPS)	NET-08.2	Mechanisms exist to utilize Wireless Intrusion Detection / Protection Systems (WIDS / WIPS) on wireless network segments.							SI-04(15)										
SI	SI-04(16)	SI-4(16)	System Monitoring | Correlate Monitoring Information	Correlate information from monitoring tools and mechanisms employed throughout the system	SI-4(16)	Not Selected	Functional	Equal	10	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance						SI-04(16)	SI-04(16)									SI-04(16)	
SI	SI-04(17)	SI-4(17)	System Monitoring | Integrated Situational Awareness	and supply chain activities to achieve integrated,	SI-4(17)	Not Selected	Functional	Equal	10	Integration of Scanning & Other Monitoring Information	MON-02.3	Automated mechanisms exist to correlate the analysis of vulnerability scans with the analysis of other monitoring data (e.g., network device logs, network performance, system monitoring and other sources to further enhance the ability to											SI-4(17)	SI-4(17)					
SI	SI-04(18)	SI-4(18)	System Monitoring | Analyze Traffic and Covert Exfiltration	points to detect covert exfiltration of information:	SI-4(18)	Not Selected	Functional	Intersects With	5	Data Loss Prevention (DLP)	NET-17	Automated mechanisms exist to implement Data Loss Prevention (DLP) to protect sensitive information as it is stored, transmitted and processed.	SI-4(18)	SI-4(18)	SI-4(18)	SI-4(18)	SI-04(18)	SI-04(18)	SI-04(18)	SI-04(18)	SI-4(18)	SI-4(18)	SI-4(18)	SI-4(18)	SI-4(18)					
SI	SI-04(18)	SI-4(18)	System Monitoring | Analyze Traffic and Covert Exfiltration	points to detect covert exfiltration of information:	SI-4(18)	Not Selected	Functional	Intersects With	5	Analyze Traffic for Covert Exfiltration	MON-11.1	Automated mechanisms exist to analyze network traffic to detect covert data exfiltration.	SI-4(18)	SI-4(18)	SI-4(18)	SI-4(18)	SI-04(18)	SI-04(18)	SI-04(18)	SI-04(18)	SI-4(18)	SI-4(18)	SI-4(18)	SI-4(18)	SI-4(18)					
SI	SI-04(19)	SI-4(19)	System Monitoring | Risk for Individuals	monitoring) of individuals who have been identified by	SI-4(19)	Not Selected	Functional	Equal	10	Individuals Posing Greater Risk	MON-01.14	Mechanisms exist to implement enhanced activity monitoring for individuals who have been identified as posing an increased level of risk.							SI-04(19)							SI-4(19)	SI-4(19)			SI-04(19)
SI	SI-04(20)	SI-4(20)	System Monitoring | Privileged Users	privileged users: [Assignment: organization-defined	SI-4(20)	High	Functional	Equal	10	Privileged User Oversight	MON-01.15	Mechanisms exist to implement enhanced activity monitoring for privileged users.			SI-4(20)				SI-04(20)										SI-04(20)
SI	SI-04(21)	SI-4(21)	System Monitoring | Probationary Periods	individuals during [Assignment: organization-defined	SI-4(21)	Not Selected	Functional	Equal	10	Probationary Periods	HRS-02.2	Mechanisms exist to identify newly onboarded personnel for enhanced monitoring during their probationary period.																		
SI	SI-04(22)	SI-4(22)	System Monitoring | Unauthorized Network Services	defined authorization or approval processes]; and\b.	SI-4(22)	High	Functional	Equal	10	Unauthorized Network Services	MON-11.2	Automated mechanisms exist to detect unauthorized network services and alert incident response personnel.			SI-4(22)				SI-04(22)										SI-04(22)
SI	SI-04(23)	SI-4(23)	System Monitoring | Host-based Devices	mechanisms at [Assignment: organization-defined system components]: [Assignment: organization-defined	SI-4(23)	Not Selected	Functional	Equal	10	Host-Based Devices	MON-01.6	Mechanisms exist to utilize a host-based monitoring solution to generate alerts and reports on network traffic, unauthorized changes to system configurations, attempts to bypass or turn off security safeguards and unauthorized						SI-04(23)	SI-04(23)								SI-04(23)		SI-04(23)
SI	SI-04(24)	SI-4(24)	System Monitoring | Indicators of Compromise	organization-defined list of compromise or potential	SI-4(24)	Not Selected	Functional	Intersects With	5	Monitoring for Indicators of Compromise (IOC)	MON-11.3	Automated mechanisms exist to identify and alert on Indicators of Compromise (IoC).	SI-4(24)	SI-4(24)	SI-4(24)	SI-4(24)	SI-04(24)	SI-04(24)	SI-04(24)	SI-04(24)	SI-4(24)	SI-4(24)	SI-4(24)	SI-4(24)	SI-4(24)					
SI	SI-04(24)	SI-4(24)	System Monitoring | Indicators of Compromise	compromise provided by [Assignment: organization-defined sources] to identify [Assignment: organization-defined list of compromise or potential compromise	SI-4(24)	Not Selected	Functional	Intersects With	5	File Integrity Monitoring (FIM)	MON-01.7	Mechanisms exist to utilize a File Integrity Monitor (FIM), or similar change-detection technology, on critical Technology Assets, Applications and/or Services (TAAS) to generate alerts for unauthorized	SI-4(24)	SI-4(24)	SI-4(24)	SI-4(24)	SI-04(24)	SI-04(24)	SI-04(24)	SI-04(24)	SI-4(24)	SI-4(24)	SI-4(24)	SI-4(24)	SI-4(24)					
SI	SI-04(25)	SI-4(25)	System Monitoring | Optimize Network Traffic Analysis	internal system interfaces to optimize the effectiveness	SI-4(25)	Not Selected	Functional	Intersects With	5	Limit Network Connections	NET-03.1	Mechanisms exist to limit the number of concurrent external network connections to its Technology Assets, Applications and/or Services (TAAS).	SI-4(25)	SI-4(25)	SI-4(25)	SI-4(25)	SI-04(25)	SI-04(25)	SI-04(25)	SI-04(25)	SI-4(25)	SI-4(25)	SI-4(25)	SI-4(25)	SI-4(25)					
SI	SI-04(25)	SI-4(25)	System Monitoring | Optimize Network Traffic Analysis	internal system interfaces to optimize the effectiveness	SI-4(25)	Not Selected	Functional	Intersects With	5	Intrusion Detection & Prevention Systems (IDS & IPS)	MON-01.1	Mechanisms exist to implement Intrusion Detection / Prevention Systems (IDS / IPS) technologies on critical systems, key network segments and network choke points.	SI-4(25)	SI-4(25)	SI-4(25)	SI-4(25)	SI-04(25)	SI-04(25)	SI-04(25)	SI-04(25)	SI-4(25)	SI-4(25)	SI-4(25)	SI-4(25)	SI-4(25)					
SI	SI-05	SI-5	Security Alerts, Advisories, and Directives	[Assignment: organization-defined personnel or roles];	SI-5	Low	Functional	Intersects With	5	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	SI-5	SI-5	SI-5	SI-5	SI-05	SI-05	SI-05	SI-05	SI-5	SI-5	SI-5	SI-5	SI-5	SI-05	SI-05	SI-05	SI-05	SI-05
SI	SI-05	SI-5	Security Alerts, Advisories, and Directives	[Assignment: organization-defined personnel or roles];	SI-5	Low	Functional	Intersects With	5	Threat Intelligence Feeds Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving cyber threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	SI-5	SI-5	SI-5	SI-5	SI-05	SI-05	SI-05	SI-05	SI-5	SI-5	SI-5	SI-5	SI-5	SI-05	SI-05	SI-05	SI-05	SI-05
SI	SI-05	SI-5	Security Alerts, Advisories, and Directives	[Assignment: organization-defined personnel or roles];	SI-5	Low	Functional	Intersects With	5	Safeguarding Data Over Open Networks	NET-12	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.	SI-5	SI-5	SI-5	SI-5	SI-05	SI-05	SI-05	SI-05	SI-5	SI-5	SI-5	SI-5	SI-5	SI-05	SI-05	SI-05	SI-05	SI-05
SI	SI-05(01)	SI-5(1)	Security Alerts, Advisories, and Directives | Automated Alerts and Advisories	[Assignment: organization-defined personnel or roles];	SI-5(1)	High	Functional	Intersects With	5	Threat Intelligence Feeds Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving cyber threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the				SI-5(1)				SI-05(01)										SI-05(01)
SI	SI-06	SI-6	Security and Privacy Function Verification	user with appropriate privilege: [Assignment: organization-defined frequency](c. Alert [Assignment:	SI-6	High	Functional	Intersects With	5	Control Functionality Verification	CHG-06	Mechanisms exist to verify the functionality of cybersecurity and/or data privacy controls following implemented changes to ensure applicable controls operate as designed.			SI-6			SI-06	SI-06								SI-06		
SI	SI-06(01)	SI-6(1)		Withdrawn	SI-6(1)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
SI	SI-06(02)	SI-6(2)	Security and Privacy Function Verification | Automation Support for Distributed Testing	management of distributed security and privacy function	SI-6(2)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SI	SI-06(03)	SI-6(3)	Security and Privacy Function Verification | Report Verification Results	verification to [Assignment: organization-defined	SI-6(3)	Not Selected	Functional	Equal	10	Report Verification Results	CHG-06.1	Mechanisms exist to report the results of cybersecurity and data protection function verification to appropriate organizational management.																		
SI	SI-07	SI-7	Software, Firmware, and Information Integrity	defined software, firmware, and information]; andb.	SI-7	Moderate	Functional	Intersects With	5	Endpoint File Integrity Monitoring (FIM)	END-06	Mechanisms exist to utilize File Integrity Monitor (FIM), or similar technologies, to detect and report on unauthorized changes to selected files and configuration settings.	SI-7	SI-7	SI-7	SI-7	SI-07	SI-07	SI-07	SI-07	SI-7	SI-7	SI-7	SI-7	SI-7	SI-07	SI-07	SI-07	SI-07	SI-07
SI	SI-07	SI-7	Software, Firmware, and Information Integrity	defined software, firmware, and information]; andb.	SI-7	Moderate	Functional	Intersects With	5	Safeguarding Data Over Open Networks	NET-12	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.	SI-7	SI-7	SI-7	SI-7	SI-07	SI-07	SI-07	SI-07	SI-7	SI-7	SI-7	SI-7	SI-7	SI-07	SI-07	SI-07	SI-07	SI-07
SI	SI-07	SI-7	Software, Firmware, and Information Integrity	defined software, firmware, and information]; andb.	SI-7	Moderate	Functional	Intersects With	5	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	SI-7	SI-7	SI-7	SI-7	SI-07	SI-07	SI-07	SI-07	SI-7	SI-7	SI-7	SI-7	SI-7	SI-07	SI-07	SI-07	SI-07	SI-07
SI	SI-07(01)	SI-7(1)	Software, Firmware, and Information Integrity | Integrity Checks	one or more): at startup; at [Assignment: organization-	SI-7(1)	Moderate	Functional	Equal	10	Integrity Checks	END-06.1	Mechanisms exist to validate configurations through integrity checking of software and firmware.		SI-7(1)	SI-7(1)			SI-07(01)	SI-07(01)									SI-07(01)	
SI	SI-07(02)	SI-7(2)	Software, Firmware, and Information Integrity | Automated Notifications of Integrity Violations	[Assignment: organization-defined personnel or roles] upon discovering discrepancies during integrity	SI-7(2)	High	Functional	Equal	10	Automated Notifications of Integrity Violations	END-06.3	Automated mechanisms exist to alert incident response personnel upon discovering discrepancies during integrity verification.			SI-7(2)				SI-07(02)										SI-07(02)
SI	SI-07(03)	SI-7(3)	Software, Firmware, and Information Integrity | Centrally Managed Integrity Tools	Employ centrally managed integrity verification tools.	SI-7(3)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SI	SI-07(04)	SI-7(4)		Withdrawn	SI-7(4)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
SI	SI-07(05)	SI-7(5)	Software, Firmware, and Information Integrity | Automated Response to Integrity Violations	down; restart the system; implement [Assignment: organization-defined controls]] when integrity violations	SI-7(5)	High	Functional	Equal	10	Automated Response to Integrity Violations	END-06.4	Automated mechanisms exist to implement remediation actions when integrity violations are discovered.			SI-7(5)				SI-07(05)										SI-07(05)
SI	SI-07(06)	SI-7(6)	Software, Firmware, and Information Integrity | Cryptographic Protection	unauthorized changes to software, firmware, and	SI-7(6)	Not Selected	Functional	Equal	10	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.																		
SI	SI-07(07)	SI-7(7)	Software, Firmware, and Information Integrity | Integration of Detection and Response	changes into the organization's incident response capability: [Assignment: organization-defined security	SI-7(7)	Moderate	Functional	Equal	10	Endpoint Detection & Response (EDR)	END-06.2	Mechanisms exist to detect and respond to unauthorized configuration changes as cybersecurity incidents.		SI-7(7)	SI-7(7)			SI-07(07)	SI-07(07)							SI-07(07)	SI-07(07)	SI-07(07)	
SI	SI-07(08)	SI-7(8)	Software, Firmware, and Information Integrity | Auditing Capability for Significant Events	following actions: [Selection (one or more): generate an audit record; alert current user; alert [Assignment:	SI-7(8)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SI	SI-07(09)	SI-7(9)	Software, Firmware, and Information Integrity | Verify Boot Process	system components: [Assignment: organization-defined	SI-7(9)	Not Selected	Functional	Equal	10	Boot Process Integrity	END-06.5	Automated mechanisms exist to verify the integrity of the boot process of systems.																		
SI	SI-07(10)	SI-7(10)	Software, Firmware, and Information Integrity | Protection of Boot Firmware	integrity of boot firmware in [Assignment: organization-defined system components]: [Assignment:	SI-7(10)	Not Selected	Functional	Equal	10	Protection of Boot Firmware	END-06.6	Automated mechanisms exist to protect the integrity of boot firmware in systems.																		
SI	SI-07(11)	SI-7(11)		Withdrawn	SI-7(11)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
SI	SI-07(12)	SI-7(12)	Software, Firmware, and Information Integrity | Integrity Verification	software be verified prior to execution: [Assignment:	SI-7(12)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SI	SI-07(13)	SI-7(13)		Withdrawn	SI-7(13)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
SI	SI-07(14)	SI-7(14)		Withdrawn	SI-7(14)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A														SI-7(14)	SI-7(14)			SI-07(14)
SI	SI-07(15)	SI-7(15)	Software, Firmware, and Information Integrity | Code Authentication	the following software or firmware components prior to	SI-7(15)	High	Functional	Intersects With	5	Signed Components	CHG-04.2	Mechanisms exist to prevent the installation of software and firmware components without verification that the component has been digitally signed using an organization-approved certificate authority.			SI-7(15)				SI-07(15)					SI-7(15)					
SI	SI-07(16)	SI-7(16)	Software, Firmware, and Information Integrity | Time Limit on Process Execution Without Supervision	for more than [Assignment: organization-defined time	SI-7(16)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SI	SI-07(17)	SI-7(17)	Software, Firmware, and Information Integrity | Runtime Application Self-protection	Implement [Assignment: organization-defined controls] for application self-protection at runtime.	SI-7(17)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SI	SI-08	SI-8	Spam Protection	messages; and\b. Update spam protection mechanisms	SI-8	Moderate	Functional	Equal	10	Phishing & Spam Protection	END-08	Mechanisms exist to utilize anti-phishing and spam protection technologies to detect and take action on unsolicited messages transported by electronic mail.		SI-8	SI-8			SI-08	SI-08							SI-08	SI-08		SI-08
SI	SI-08(01)	SI-8(1)		Withdrawn	SI-8(1)	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
SI	SI-08(02)	SI-8(2)	Spam Protection | Automatic Updates	Automatically update spam protection mechanisms [Assignment: organization-defined frequency];	SI-8(2)	Moderate	Functional	Equal	10	Automatic Spam and Phishing Protection Updates	END-08.2	Mechanisms exist to automatically update anti-phishing and spam protection technologies when new releases are available in accordance with configuration and change management practices.		SI-8(2)	SI-8(2)			SI-08(02)	SI-08(02)								SI-08(02)		SI-08(02)
SI	SI-08(03)	SI-8(3)	Spam Protection | Continuous Learning Capability	capability to more effectively identify legitimate	SI-8(3)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SI	SI-09	SI-9		Withdrawn	SI-9	Withdrawn	Functional	No Relationship	0	N/A	N/A	N/A																		
SI	SI-10	SI-10	Information Input Validation	[Assignment: organization-defined information inputs to	SI-10	Moderate	Functional	Intersects With	5	Safeguarding Data Over Open Networks	NET-12	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.	SI-10	SI-10	SI-10	SI-10	SI-10	SI-10	SI-10	SI-10	SI-10	SI-10	SI-10	SI-10	SI-10	SI-10	SI-10	SI-10	SI-10	SI-10
SI	SI-10	SI-10	Information Input Validation	[Assignment: organization-defined information inputs to	SI-10	Moderate	Functional	Intersects With	5	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	SI-10	SI-10	SI-10	SI-10	SI-10	SI-10	SI-10	SI-10	SI-10	SI-10	SI-10	SI-10	SI-10	SI-10	SI-10	SI-10	SI-10	SI-10
SI	SI-10(01)	SI-10(1)	Information Input Validation | Manual Override Capability	base control (SI-10)]:b. Restrict the use of the manual	SI-10(1)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SI	SI-10(02)	SI-10(2)	Information Input Validation | Review and Resolve Errors	Review and resolve input validation errors within [Assignment: organization-defined time period];	SI-10(2)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SI	SI-10(03)	SI-10(3)	Information Input Validation | Predictable Behavior	Verify that the system behaves in a predictable and documented manner when invalid inputs are received.	SI-10(3)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SI	SI-10(04)	SI-10(4)	Information Input Validation | Timing Interactions	components in determining appropriate responses for	SI-10(4)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SI	SI-10(05)	SI-10(5)	Information Input Validation | Restrict Inputs to Trusted Sources and Approved Formats	organization-defined trusted sources] and/or	SI-10(5)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SI	SI-10(06)	SI-10(6)	Information Input Validation | Injection Prevention	Prevent untrusted data injections.	SI-10(6)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																		
SI	SI-11	SI-11	Error Handling	information that could be exploited by adversaries;	SI-11	Moderate	Functional	Equal	10	Error Handling	TDA-19	(2) Generating error messages that provide information necessary for corrective actions without revealing sensitive or potentially harmful information in error logs and administrative messages that		SI-11	SI-11				SI-11	SI-11							SI-11	SI-11		SI-11
SI	SI-12	SI-12	Information Management and Retention	applicable laws, executive orders, directives,	SI-12	Low	Functional	Intersects With	5	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	SI-12	SI-12	SI-12	SI-12	SI-12	SI-12	SI-12	SI-12	SI-12	SI-12	SI-12	SI-12	SI-12	SI-12	SI-12	SI-12	SI-12	SI-12
SI	SI-12	SI-12	Information Management and Retention	applicable laws, executive orders, directives,	SI-12	Low	Functional	Intersects With	5	Personal Data Retention & Disposal	PRI-05	(2) Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of storage; and	SI-12	SI-12	SI-12	SI-12	SI-12	SI-12	SI-12	SI-12	SI-12	SI-12	SI-12	SI-12	SI-12	SI-12	SI-12	SI-12	SI-12	SI-12
SI	SI-12(01)	SI-12(1)	Information Management and Retention | Limit Personally Identifiable Information Elements	Limit personally identifiable information being	SI-12(1)	Not Selected	Functional	Intersects With	5	Internal Use of Personal Data For Testing, Training and Research	PRI-05.1	(1) Takes measures to limit or minimize the amount of PD used for internal testing, training and research purposes; and	SI-12(1)	SI-12(1)	SI-12(1)	SI-12(1)	SI-12(01)	SI-12(01)	SI-12(01)	SI-12(01)	SI-12(1)	SI-12(1)	SI-12(1)	SI-12(1)	SI-12(1)					
SI	SI-12(01)	SI-12(1)	Information Management and Retention | Limit Personally Identifiable Information Elements	personally identifiable information being	SI-12(1)	Not Selected	Functional	Intersects With	5	Minimize Sensitive / Regulated Data	D

Family	Sorting Control #	Focal Document Element	Focal Document Element Name	Focal Document Element Description	NIST SP 800-53 R5.2	Security Control Baseline	Set Theory Relationship Mapping (STRM)			Reference Document Element	Reference Document Element Name	Reference Document Element Description	NIST SP 800-53 R5.2 Baselines				FedRAMP R5				NIST SP 800-161 R1					GovRAMP				
							Rationale	Relationship	Strength of Relationship				Low	Mod	High	Privacy	Low	Mod	High	LI-SaaS	C-SCRM Baseline	Low Impact Software	Level 1	Level 2	Level 3	Low	Low+	Moderate	Core	High (FedRAMP Tailored)
SI	SI-14(03)	SI-14(3)	Non-persistence | Non-persistent Connectivity	Establish connections to the system on demand and terminate connections after [Selection (one): completion of a request; a period of non-use].	SI-14(3)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
SI	SI-15	SI-15	Information Output Filtering	Validate information output from [Assignment: organization-defined software programs and/or applications] to ensure that the information is consistent with the expected content.	SI-15	Not Selected	Functional	Equal	10	Information Output Filtering	SEA-09	Mechanisms exist to validate information output from software programs and/or applications to ensure that the information is consistent with the expected content.																	
SI	SI-16	SI-16	Memory Protection	Implement [Assignment: organization-defined security safeguards] to protect its memory from unauthorized code execution.	SI-16	Moderate	Functional	Equal	10	Memory Protection	SEA-10	Mechanisms exist to implement security safeguards to protect system memory from unauthorized code execution.		SI-16	SI-16			SI-16	SI-16						SI-16	SI-16	SI-16		SI-16
SI	SI-17	SI-17	Fail-safe Procedures	Implement the following fail-safe procedures when the following failures occur: [Assignment: organization-defined list of failure conditions and associated fail-safe procedures].	SI-17	Not Selected	Functional	Equal	10	Fail Safe	SEA-07.3	Mechanisms exist to implement fail-safe procedures when failure conditions occur.																	
SI	SI-18	SI-18	Personally Identifiable Information Quality Operations	Check the accuracy, relevance, timeliness, impact, completeness and de-identification of information across the information lifecycle [Assignment: organization-defined frequency], and correct or delete inaccurate or outdated personally identifiable information.	SI-18	Not Selected	Functional	Intersects With	5	Data Quality Operations	DCH-22	Mechanisms exist to check the accuracy, relevance, timeliness, impact, completeness and de-identification of information throughout the information lifecycle.				SI-18													
SI	SI-18(01)	SI-18(1)	Personally Identifiable Information Quality Operations | Automation Support	Correct or delete personally identifiable information that is inaccurate or outdated, incorrectly determined regarding impact, or incorrectly de-identified using [Assignment: organization-defined automated mechanisms].	SI-18(1)	Not Selected	Functional	Intersects With	5	Data Quality Operations	DCH-22	Mechanisms exist to check the accuracy, relevance, timeliness, impact, completeness and de-identification of information throughout the information lifecycle.																	
SI	SI-18(02)	SI-18(2)	Personally Identifiable Information Quality Operations | Data Tags	Employ data tags to automate the correction or deletion of personally identifiable information across the information lifecycle.	SI-18(2)	Not Selected	Functional	Equal	10	Data Tags	DCH-22.2	Mechanisms exist to utilize data tags to automate tracking of sensitive/regulated data across the information lifecycle.																	
SI	SI-18(03)	SI-18(3)	Personally Identifiable Information Quality Operations | Collection	Collect personally identifiable information directly from the individual.	SI-18(3)	Not Selected	Functional	Equal	10	Primary Source Personal Data (PD) Collection	DCH-22.3	Mechanisms exist to collect Personal Data (PD) directly from the individual.																	
SI	SI-18(04)	SI-18(4)	Personally Identifiable Information Quality Operations | Individual Requests	Correct personally identifiable information upon request by individuals or their designated representatives.	SI-18(4)	Not Selected	Functional	Intersects With	5	Correcting Inaccurate Personal Data	PRI-06.1	(1) Data subjects to have inaccurate Personal Data (PD) maintained by the organization corrected or amended; and	SI-18(4)	SI-18(4)	SI-18(4)	SI-18(4)	SI-18(04)	SI-18(04)	SI-18(04)	SI-18(04)	SI-18(4)	SI-18(4)	SI-18(4)	SI-18(4)	SI-18(4)					
SI	SI-18(04)	SI-18(4)	Personally Identifiable Information Quality Operations | Individual Requests	Correct personally identifiable information upon request by individuals or their designated representatives.	SI-18(4)	Not Selected	Functional	Intersects With	5	Updating & Correcting Personal Data (PD)	DCH-22.1	Mechanisms exist to utilize technical controls to correct Personal Data (PD) that is inaccurate or outdated, incorrectly determined regarding impact, or incorrectly de-identified.	SI-18(4)	SI-18(4)	SI-18(4)	SI-18(4)	SI-18(04)	SI-18(04)	SI-18(04)	SI-18(04)	SI-18(4)	SI-18(4)	SI-18(4)	SI-18(4)	SI-18(4)					
SI	SI-18(04)	SI-18(4)	Personally Identifiable Information Quality Operations | Individual Requests	Correct personally identifiable information upon request by individuals or their designated representatives.	SI-18(4)	Not Selected	Functional	Intersects With	5	Data Subject Empowerment	PRI-06	(3) Disseminate the corrections or amendments to the Personal Data (PD) to all authorized recipients that received the inaccurate PD that was transmitted, shared, updated and/or disposed;	SI-18(4)	SI-18(4)	SI-18(4)	SI-18(4)	SI-18(04)	SI-18(04)	SI-18(04)	SI-18(04)	SI-18(4)	SI-18(4)	SI-18(4)	SI-18(4)	SI-18(4)					
SI	SI-18(05)	SI-18(5)	Personally Identifiable Information Quality Operations | Notice of Correction or Deletion	Notify [Assignment: organization-defined recipients of personally identifiable information] and individuals that the personally identifiable information has been corrected or deleted.	SI-18(5)	Not Selected	Functional	Intersects With	5	Updating & Correcting Personal Data (PD)	DCH-22.1	(3) Obtain the source(s) of their PD;	SI-18(5)	SI-18(5)	SI-18(5)	SI-18(5)	SI-18(05)	SI-18(05)	SI-18(05)	SI-18(05)	SI-18(5)	SI-18(5)	SI-18(5)	SI-18(5)	SI-18(5)					
SI	SI-18(05)	SI-18(5)	Personally Identifiable Information Quality Operations | Notice of Correction or Deletion	Notify [Assignment: organization-defined recipients of personally identifiable information] and individuals that the personally identifiable information has been corrected or deleted.	SI-18(5)	Not Selected	Functional	Intersects With	5	Correcting Inaccurate Personal Data	PRI-06.1	Mechanisms exist to utilize technical controls to correct Personal Data (PD) that is inaccurate or outdated, incorrectly determined regarding impact, or incorrectly de-identified.	SI-18(5)	SI-18(5)	SI-18(5)	SI-18(5)	SI-18(05)	SI-18(05)	SI-18(05)	SI-18(05)	SI-18(5)	SI-18(5)	SI-18(5)	SI-18(5)	SI-18(5)					
SI	SI-18(05)	SI-18(5)	Personally Identifiable Information Quality Operations | Notice of Correction or Deletion	Notify [Assignment: organization-defined recipients of personally identifiable information] and individuals that the personally identifiable information has been corrected or deleted.	SI-18(5)	Not Selected	Functional	Intersects With	5	Notice of Correction or Processing Change	PRI-06.2	(1) Data subjects to have inaccurate Personal Data (PD) maintained by the organization corrected or amended; and (2) Disseminate notice of the corrected or amended PD to all authorized recipients that received the inaccurate PD that was transmitted, shared, updated and/or disposed;	SI-18(5)	SI-18(5)	SI-18(5)	SI-18(5)	SI-18(05)	SI-18(05)	SI-18(05)	SI-18(05)	SI-18(5)	SI-18(5)	SI-18(5)	SI-18(5)	SI-18(5)					
SI	SI-19	SI-19	De-identification	Remove the following information from datasets: [Assignment: organization-defined information]; and Use the following techniques to remove the information: [Assignment: organization-defined techniques].	SI-19	Not Selected	Functional	Equal	10	De-Identification (Anonymization)	DCH-23	Mechanisms exist to anonymize data by removing Personal Data (PD) from datasets.								SI-19									
SI	SI-19(01)	SI-19(1)	De-identification | Collection	De-identify the dataset upon collection by not collecting personally identifiable information.	SI-19(1)	Not Selected	Functional	Intersects With	5	Primary Source Personal Data (PD) Collection	DCH-22.3	Mechanisms exist to collect Personal Data (PD) directly from the individual.	SI-19(1)	SI-19(1)	SI-19(1)	SI-19(1)	SI-19(01)	SI-19(01)	SI-19(01)	SI-19(01)	SI-19(1)	SI-19(1)	SI-19(1)	SI-19(1)	SI-19(1)					
SI	SI-19(01)	SI-19(1)	De-identification | Collection	De-identify the dataset upon collection by not collecting personally identifiable information.	SI-19(1)	Not Selected	Functional	Intersects With	5	De-Identify Dataset Upon Collection	DCH-23.1	Mechanisms exist to de-identify the dataset upon collection by not collecting Personal Data (PD).	SI-19(1)	SI-19(1)	SI-19(1)	SI-19(1)	SI-19(01)	SI-19(01)	SI-19(01)	SI-19(01)	SI-19(1)	SI-19(1)	SI-19(1)	SI-19(1)	SI-19(1)					
SI	SI-19(02)	SI-19(2)	De-identification | Archiving	Prohibit archiving of personally identifiable information elements if those elements in a dataset will not be needed after the dataset is archived.	SI-19(2)	Not Selected	Functional	Equal	10	Archiving	DCH-23.2	Mechanisms exist to refrain from archiving Personal Data (PD) elements if those elements in a dataset will not be needed after the dataset is archived.																	
SI	SI-19(03)	SI-19(3)	De-identification | Release	Remove personally identifiable information elements from a dataset prior to its release if those elements in the dataset do not need to be part of the data release.	SI-19(3)	Not Selected	Functional	Equal	10	Release	DCH-23.3	Mechanisms exist to remove Personal Data (PD) elements from a dataset prior to its release if those elements in the dataset do not need to be part of the data release.																	
SI	SI-19(04)	SI-19(4)	De-identification | Removal, Masking, Encryption, Hashing, or Replacement of Direct Identifiers	Remove, mask, encrypt, hash, or replace direct identifiers in a dataset.	SI-19(4)	Not Selected	Functional	Intersects With	5	Data Masking	PRI-05.3	Mechanisms exist to mask sensitive/regulated data through data anonymization, pseudonymization, redaction or de-identification.	SI-19(4)	SI-19(4)	SI-19(4)	SI-19(4)	SI-19(04)	SI-19(04)	SI-19(04)	SI-19(04)	SI-19(4)	SI-19(4)	SI-19(4)	SI-19(4)	SI-19(4)					
SI	SI-19(04)	SI-19(4)	De-identification | Removal, Masking, Encryption, Hashing, or Replacement of Direct Identifiers	Remove, mask, encrypt, hash, or replace direct identifiers in a dataset.	SI-19(4)	Not Selected	Functional	Intersects With	5	Removal, Masking, Encryption, Hashing or Replacement of Direct Identifiers	DCH-23.4	Mechanisms exist to remove, mask, encrypt, hash or replace direct identifiers in a dataset.	SI-19(4)	SI-19(4)	SI-19(4)	SI-19(4)	SI-19(04)	SI-19(04)	SI-19(04)	SI-19(04)	SI-19(4)	SI-19(4)	SI-19(4)	SI-19(4)	SI-19(4)					
SI	SI-19(05)	SI-19(5)	De-identification | Statistical Disclosure Control	Manipulate numerical data, contingency tables, and statistical findings so that no individual or organization is identifiable in the results of the analysis.	SI-19(5)	Not Selected	Functional	Equal	10	Statistical Disclosure Control	DCH-23.5	Mechanisms exist to manipulate numerical data, contingency tables and statistical findings so that no person or organization is identifiable in the results of the analysis.																	
SI	SI-19(06)	SI-19(6)	De-identification | Differential Privacy	Prevent disclosure of personal data by adding non-deterministic noise to the results of mathematical operations before the results are reported.	SI-19(6)	Not Selected	Functional	Equal	10	Differential Data Privacy	DCH-23.6	Mechanisms exist to prevent disclosure of Personal Data (PD) by adding non-deterministic noise to the results of mathematical operations before the results are reported.																	
SI	SI-19(07)	SI-19(7)	De-identification | Validated Algorithms and Software	Perform de-identification using validated algorithms and software that is validated to implement the algorithms.	SI-19(7)	Not Selected	Functional	Equal	10	Automated De-Identification of Sensitive Data	DCH-23.7	Mechanisms exist to perform de-identification of sensitive/regulated data, using validated algorithms and software to implement the algorithms.																	
SI	SI-19(08)	SI-19(8)	De-identification | Motivated Intruder	Perform a motivated intruder test on the de-identified dataset to determine if the identified data remains or if re-identification can be performed.	SI-19(8)	Not Selected	Functional	Equal	10	Motivated Intruder	DCH-23.8	Mechanisms exist to perform a motivated intruder test on the de-identified dataset to determine if the identified data remains or if the de-identified data can be re-identified.																	
SI	SI-20	SI-20	Tainting	Embed data or capabilities in the following systems or system components to determine if organizational data has been exfiltrated or improperly removed from the organization: [Assignment: organization-defined systems or system components].	SI-20	Not Selected	Functional	Equal	10	Tainting	THR-08	Mechanisms exist to embed false data or steganographic data in files to enable the organization to determine if data has been exfiltrated and provide a means to identify the individual(s) involved.									SI-20			SI-20	SI-20					
SI	SI-21	SI-21	Information Refresh	Refresh [Assignment: organization-defined information] at [Assignment: organization-defined frequencies] or generate the information on demand and delete the information when no longer needed.	SI-21	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
SI	SI-22	SI-22	Information Diversity	Identify the following alternative sources for the [Assignment: organization-defined information]; and Distribute the [Assignment: organization-defined information] across the implementation of the supply chain risk management policy and the associated supply chain risk management plan.	SI-22	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
SI	SI-23	SI-23	Information Fragmentation	Implement the following supply chain risk management policy and the associated supply chain risk management plan: [Assignment: organization-defined policies and procedures].	SI-23	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
SR	SR-01	SR-1	Policy and Procedures	Develop, maintain, and disseminate to [Assignment: organization-defined personnel or roles]:	SR-1	Low	Functional	Intersects With	5	Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their	SR-1	SR-1	SR-1	SR-1	SR-01	SR-01	SR-01	SR-01	SR-1	SR-1	SR-1	SR-1	SR-1					
SR	SR-01	SR-1	Policy and Procedures	Develop, maintain, and disseminate to [Assignment: organization-defined personnel or roles]:	SR-1	Low	Functional	Subset Of	10	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	SR-1	SR-1	SR-1	SR-1	SR-01	SR-01	SR-01	SR-01	SR-1	SR-1	SR-1	SR-1	SR-1					
SR	SR-01	SR-1	Policy and Procedures	Develop, maintain, and disseminate to [Assignment: organization-defined personnel or roles]:	SR-1	Low	Functional	Subset Of	10	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	SR-1	SR-1	SR-1	SR-1	SR-01	SR-01	SR-01	SR-01	SR-1	SR-1	SR-1	SR-1	SR-1					
SR	SR-02	SR-2	Supply Chain Risk Management Plan	Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the following systems, system components, or system services: [Assignment: organization-defined systems, system components, or system services];	SR-2	Low	Functional	Intersects With	5	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services	SR-2	SR-2	SR-2	SR-2	SR-02	SR-02	SR-02	SR-02	SR-2	SR-2	SR-2	SR-2	SR-2					
SR	SR-02	SR-2	Supply Chain Risk Management Plan	Review and update the supply chain risk management plan [Assignment: organization-defined frequency] or as required, to address threat, organizational or environmental changes; and	SR-2	Low	Functional	Intersects With	5	Supply Chain Risk Management (SCRM) Plan	TPM-03	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services	SR-2	SR-2	SR-2	SR-2	SR-02	SR-02	SR-02	SR-02	SR-2	SR-2	SR-2	SR-2	SR-2					
SR	SR-02(01)	SR-2(1)	Supply Chain Risk Management Plan | Establish SCRM Team	Establish a supply chain risk management team consisting of [Assignment: organization-defined personnel, roles, and responsibilities] to lead and support the following SCRM activities: [Assignment: organization-defined supply chain risk management activities].	SR-2(1)	Low	Functional	Intersects With	5	Supply Chain Risk Management (SCRM) Plan	TPM-03	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services	SR-2(1)	SR-2(1)	SR-2(1)		SR-02(01)	SR-02(01)	SR-02(01)	SR-02(01)										
SR	SR-03	SR-3	Supply Chain Controls and Processes	Establish a process or processes to identify [Assignment: organization-defined supply chain elements, processes, and actors] for the following systems, system components, or system services: [Assignment: organization-defined systems, system components, or system services]; and	SR-3	Low	Functional	Equal	10	Processes To Address Weaknesses or Deficiencies	TPM-03.3	Mechanisms exist to address identified weaknesses or deficiencies in the security of the supply chain	SR-3	SR-3	SR-3		SR-03	SR-03	SR-03	SR-03	SR-3		SR-3	SR-3	SR-3					
SR	SR-03(01)	SR-3(1)	Supply Chain Controls and Processes | Diverse Supply Base	Employ a diverse set of sources for the following system components and services: [Assignment: organization-defined system components and services].	SR-3(1)	Not Selected	Functional	Intersects With	5	Development Methods, Techniques & Processes	TDA-02.3	Mechanisms exist to require software developers to ensure that their software development processes employ industry-recognized secure practices for secure programming, engineering methods, quality	SR-3(1)	SR-3(1)	SR-3(1)	SR-3(1)	SR-03(01)	SR-03(01)	SR-03(01)	SR-03(01)	SR-3(1)	SR-3(1)	SR-3(1)	SR-3(1)	SR-3(1)					
SR	SR-03(01)	SR-3(1)	Supply Chain Controls and Processes | Diverse Supply Base	Employ a diverse set of sources for the following system components and services: [Assignment: organization-defined system components and services].	SR-3(1)	Not Selected	Functional	Intersects With	5	Supplier Diversity	TDA-03.1	Mechanisms exist to obtain cybersecurity and data protection technologies from different suppliers to minimize supply chain risk.	SR-3(1)	SR-3(1)	SR-3(1)	SR-3(1)	SR-03(01)	SR-03(01)	SR-03(01)	SR-03(01)	SR-3(1)	SR-3(1)	SR-3(1)	SR-3(1)	SR-3(1)					
SR	SR-03(01)	SR-3(1)	Supply Chain Controls and Processes | Diverse Supply Base	Employ a diverse set of sources for the following system components and services: [Assignment: organization-defined system components and services].	SR-3(1)	Not Selected	Functional	Intersects With	5	Acquisition Strategies, Tools & Methods	TPM-03.1	Mechanisms exist to utilize tailored acquisition strategies, contract tools and procurement methods for the purchase of unique Technology Assets, Applications and/or Services (TAAS).	SR-3(1)	SR-3(1)	SR-3(1)	SR-3(1)	SR-03(01)	SR-03(01)	SR-03(01)	SR-03(01)	SR-3(1)	SR-3(1)	SR-3(1)	SR-3(1)	SR-3(1)					
SR	SR-03(02)	SR-3(2)	Supply Chain Controls and Processes | Limitation of Harm	Employ the following controls to limit harm from potential adversaries identifying and targeting the organization's supply chain: [Assignment: organization-defined controls].	SR-3(2)	Not Selected	Functional	Equal	10	Limit Potential Harm	TPM-03.2	Mechanisms exist to utilize security safeguards to limit harm from potential adversaries who identify and target the organization's supply chain.																	
SR	SR-03(03)	SR-3(3)	Supply Chain Controls and Processes | Sub-tier Flow Down	Ensure that the controls included in the contracts of prime contractors are also included in the contracts of subcontractors.	SR-3(3)	Not Selected	Functional	Intersects With	5	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity and data protection requirements with third-parties, reflecting the organization's needs to protect its Technology Assets,	SR-3(3)	SR-3(3)	SR-3(3)	SR-3(3)	SR-03(03)	SR-03(03)	SR-03(03)	SR-03(03)	SR-3(3)	SR-3(3)	SR-3(3)	SR-3(3)	SR-3(3)					
SR	SR-03(03)	SR-3(3)	Supply Chain Controls and Processes | Sub-tier Flow Down	Ensure that the controls included in the contracts of prime contractors are also included in the contracts of subcontractors.	SR-3(3)	Not Selected	Functional	Intersects With	5	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure cybersecurity and data protection requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	SR-3(3)	SR-3(3)	SR-3(3)	SR-3(3)	SR-03(03)	SR-03(03)	SR-03(03)	SR-03(03)	SR-3(3)	SR-3(3)	SR-3(3)	SR-3(3)	SR-3(3)					
SR	SR-04	SR-4	Provenance	Document, monitor, and maintain valid provenance of the following systems, system components, and associated data: [Assignment: organization-defined systems, system components, and associated data].	SR-4	Not Selected	Functional	Intersects With	5	Provenance	AST-03.2	Mechanisms exist to track the origin, development, ownership, location and changes to Technology Assets, Applications, Services and/or Data (TAASD).												SR-4	SR-4				
SR	SR-04(01)	SR-4(1)	Provenance | Identity	Establish and maintain unique identities for the following system components: [Assignment: organization-defined systems or system components].	SR-4(1)	Not Selected	Functional	Intersects With	5	Provenance	AST-03.2	Mechanisms exist to track the origin, development, ownership, location and changes to Technology Assets, Applications, Services and/or Data (TAASD).																	
SR	SR-04(02)	SR-4(2)	Provenance | Track and Trace	Establish and maintain unique identities for the following systems and critical system components before initiating tracking of the systems and components: [Assignment: organization-defined systems and critical system components].	SR-4(2)	Not Selected	Functional	Intersects With	5	Provenance	AST-03.2	Mechanisms exist to track the origin, development, ownership, location and changes to Technology Assets, Applications, Services and/or Data (TAASD).																	
SR	SR-04(03)	SR-4(3)	Provenance | Validate as Genuine and Not Altered	Employ the following controls to validate that the system or system component received is genuine and has not been altered: [Assignment: organization-defined controls].	SR-4(3)	Not Selected	Functional	Intersects With	5	Product Tampering and Counterfeiting (PTC)	TDA-11	Mechanisms exist to maintain the integrity and authenticity of software and data technologies and services provided by the organization throughout the supply chain by developing and implementing Product Tampering and Counterfeiting (PTC) practices that include the means to detect and prevent																	
SR	SR-04(04)	SR-4(4)	Provenance | Supply Chain Integrity — Pedigree	Employ [Assignment: organization-defined supply chain elements, processes, and actors] for the following systems, system components, or system services to ensure the integrity of the system and system components by validating the internal composition and provenance of:	SR-4(4)	Not Selected	Functional	Intersects With	5	Product Tampering and Counterfeiting (PTC)	TDA-11	Mechanisms exist to maintain the integrity and authenticity of software and data technologies and services provided by the organization throughout the supply chain by developing and implementing Product Tampering and Counterfeiting (PTC) practices that include the means to detect and prevent																	
SR	SR-05	SR-5	Acquisition Strategies, Tools, and Methods	Employ the following acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks: [Assignment: organization-defined acquisition strategies, contract tools, and procurement methods].	SR-5	Low	Functional	Intersects With	5	Acquisition Strategies, Tools & Methods	TPM-03.1	Mechanisms exist to utilize tailored acquisition strategies, contract tools and procurement methods for the purchase of unique Technology Assets, Applications and/or Services (TAAS).	SR-5	SR-5	SR-5		SR-05	SR-05	SR-05	SR-05	SR-5		SR-5	SR-5	SR-5					
SR	SR-05(01)	SR-5(1)	Acquisition Strategies, Tools, and Methods | Adequate Supply	Establish an alternate supply of [Assignment: organization-defined critical system components]; [Assignment: organization-defined actions] to be taken in the event of [Assignment: organization-defined supply disruptions].	SR-5(1)	Not Selected	Functional	Equal	10	Adequate Supply	TPM-03.4	Mechanisms exist to develop and implement a spare parts strategy to ensure that an adequate supply of critical components is available to meet operational needs.																	
SR	SR-05(02)	SR-5(2)	Acquisition Strategies, Tools, and Methods | Assessments Prior to Selection, Acceptance, Modification, or Update	Assess the following system components or system service prior to selection, acceptance, modification, or update: [Assignment: organization-defined system components or system services].	SR-5(2)	Not Selected	Functional	No Relationship	0	N/A	N/A	No applicable SCF control																	
SR	SR-06	SR-6	Supplier Assessments and Reviews	Assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide.	SR-6	Moderate	Functional	Intersects With	5	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity and data protection controls.		SR-6	SR-6			SR-06	SR-06					SR-6	SR-6				
SR	SR-06(01)	SR-6(1)	Supplier Assessments and Reviews | Testing and Analysis	Employ [Assignment: organization-defined supply chain elements, processes, and actors associated with the system, system component, or system service] to [Assignment: organization-defined actions].	SR-6(1)	Not Selected	Functional	Intersects With	5	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity and data protection controls.																	
SR	SR-07	SR-7	Supply Chain Operations Security	Implement an operations security program to protect the following system, system component, or system service: [Assignment: organization-defined systems, system components, or system services].	SR-7	Not Selected	Functional	Intersects With	5	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services	SR-7	SR-7	SR-7	SR-7	SR-07	SR-07	SR-07	SR-07	SR-7	SR-7	SR-7	SR-7	SR-7					
SR	SR-07	SR-7	Supply Chain Operations Security	Implement an operations security program to protect the following system, system component, or system service: [Assignment: organization-defined systems, system components, or system services].	SR-7	Not Selected	Functional	Intersects With	5	Operations Security	OPS-01	Mechanisms exist to facilitate the implementation of operational security controls.	SR-7	SR-7	SR-7	SR-7	SR-07	SR-07	SR-07	SR-07	SR-7	SR-7	SR-7	SR-7	SR-7					
SR	SR-08	SR-8	Notification Agreements	Establish agreements and procedures with the following entities for the component or system service for the [Selection (one or more): notification of supply chain compromises; results of assessments or audits; [Assignment: organization-defined information]]: [Assignment: organization-defined entities].	SR-8	Low	Functional	Equal	10	Security Compromise Notification Agreements	TPM-05.1	Mechanisms exist to compel External Service Providers (ESPs) to provide notification of actual or potential compromises in the supply chain that can potentially affect or have adversely affected	SR-8	SR-8	SR-8		SR-08	SR-08	SR-08	SR-08	SR-8			SR-8	SR-8					
SR	SR-09	SR-9	Tamper Resistance and Detection	Implement a tamper protection program for the system, system component, or system service.	SR-9	High	Functional	Intersects With	5	Logical Tampering Protection	AST-15	Mechanisms exist to assess the integrity of critical Technology Assets, Applications and/or Services (TAAS) to detect tampering.			SR-9									SR-9	SR-9				
SR	SR-09(01)	SR-9(1)	Tamper Resistance and Detection | Multiple Stages of System Development Life Cycle	Employ anti-tamper technologies, tools, and techniques throughout the system development life cycle.	SR-9(1)	High	Functional	Intersects With	5	Logical Tampering Protection	AST-15	Mechanisms exist to assess the integrity of critical Technology Assets, Applications and/or Services (TAAS) to detect tampering.			SR-9(1)				SR-09(01)										
SR	SR-10	SR-10	Inspection of Systems or Components	Inspect the following systems or system components [Assignment: organization-defined frequency], upon [Assignment: organization-defined indications of need for inspection]]	SR-10	Low	Functional	Intersects With	5	Product Tampering and Counterfeiting (PTC)	TDA-11	Mechanisms exist to maintain the integrity and authenticity of software and data technologies and services provided by the organization throughout the supply chain by developing and implementing Product Tampering and Counterfeiting (PTC) practices that include the means to detect and prevent	SR-10	SR-10	SR-10	SR-10	SR-10	SR-10	SR-10	SR-10	SR-10	SR-10	SR-10	SR-10	SR-10					
SR	SR-10	SR-10	Inspection of Systems or Components	Inspect the following systems or system components [Assignment: organization-defined frequency], upon [Assignment: organization-defined indications of need for inspection]]	SR-10	Low	Functional	Intersects With	5	Inspection of Systems, Components & Devices	AST-15.1	Mechanisms exist to physically and logically inspect critical technology assets to detect evidence of tampering.	SR-10	SR-10	SR-10	SR-10	SR-10	SR-10	SR-10	SR-10	SR-10	SR-10	SR-10	SR-10	SR-10					
SR	SR-11	SR-11	Component Authenticity	Develop and implement anti-counterfeit system components to detect, prevent, and report counterfeit system components.	SR-11	Low	Functional	Intersects With	5	Product Tampering and Counterfeiting (PTC)	TDA-11	Mechanisms exist to maintain the integrity and authenticity of software and data technologies and services provided by the organization throughout the supply chain by developing and implementing Product Tampering and Counterfeiting (PTC) practices that include the means to detect and prevent	SR-11	SR-11	SR-11		SR-11	SR-11	SR-11	SR-11	SR-11		SR-11	SR-11	SR-11					
SR	SR-11(01)	SR-11(1)	Component Authenticity | Anti-counterfeit Training	Train [Assignment: organization-defined personnel or roles] to detect counterfeit system components (including hardware, software, and firmware).	SR-11(1)	Low	Functional	Equal	10	Anti-Counterfeit Training	TDA-11.1	Mechanisms exist to train personnel to detect counterfeit system components, including hardware, software and firmware.	SR-11(1)	SR-11(1)	SR-11(1)		SR-11(01)	SR-11(01)	SR-11(01)	SR-11(01)	SR-11(1)			SR-11(1)	SR-11(1)					
SR	SR-11(02)	SR-11(2)	Component Authenticity | Configuration Control for Component Service and Repair	Maintain configuration control over the following system components awaiting service or repair and service or repaired components awaiting return to service: [Assignment: organization-defined system components].	SR-11(2)	Low	Functional	Equal	10	Maintain Configuration Control During Maintenance	MNT-07	Mechanisms exist to maintain proper physical security and configuration control over technology assets awaiting service or repair.	SR-11(2)	SR-11(2)	SR-11(2)		SR-11(02)	SR-11(02)	SR-11(02)	SR-11(02)	SR-11(2)			SR-11(2)	SR-11(2)					
SR	SR-11(03)	SR-11(3)	Component Authenticity | Anti-counterfeit Scanning	Scan for counterfeit system components [Assignment: organization-defined frequency].	SR-11(3)	Not Selected	Functional	Intersects With	5	Product Tampering and Counterfeiting (PTC)	TDA-11	Mechanisms exist to maintain the integrity and authenticity of software and data technologies and services provided by the organization throughout the supply chain by developing and implementing Product Tampering and Counterfeiting (PTC) practices that include the means to detect and prevent												SR-11(3)	SR-11(3)				
SR	SR-12	SR-12	Component Disposal	Dispose of [Assignment: organization-defined data, documentation, tools, or system components] using the following techniques and methods: [Assignment: organization-defined techniques and methods].	SR-12	Low	Functional	Intersects With	5	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	SR-12	SR-12	SR-12	SR-12	SR-12	SR-12	SR-12	SR-12	SR-12	SR-12	SR-12	SR-12	SR-12					