NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document Secure Controls Framework (SCF) version 2025.2
STRM Guidance: https://securecontrolsframework.com/set-theory-relationship-mapping-strm/

Focal Document: **NIST SP 800-53 Rev 5.1.1 Security and Privacy Controls for Information Systems and Organizations**
Focal Document URL: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final
Published STRM URL: https://securecontrolsframework.com/content/strm/scf-strm-general-nist-800-53-r5-1-1.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)	Low	Mod	High	Privacy
AC-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] 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:	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	NIST SP 800-53B R5 Baseline: Low	AC-1	AC-1	AC-1	AC-1
AC-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] 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:	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	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 continuing suitability, adequacy and effectiveness.	5	NIST SP 800-53B R5 Baseline: Low	AC-1	AC-1	AC-1	AC-1
AC-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] 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:	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	NIST SP 800-53B R5 Baseline: Low	AC-1	AC-1	AC-1	AC-1
AC-2	Account Management	a. Define and document the types of accounts allowed and specifically prohibited for use within the system;b. Assign account managers;c. Require [Assignment: organization-defined prerequisites and criteria] for group and role membership;d. Specify:1. Authorized users of the system;2. Group and role membership; 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	NIST SP 800-53B R5 Baseline: Low	AC-2	AC-2	AC-2	AC-2
AC-2	Account Management	a. Define and document the types of accounts allowed and specifically prohibited for use within the system;b. Assign account managers;c. Require [Assignment: organization-defined prerequisites and criteria] for group and role membership;d. Specify:1. Authorized users of the system;2. Group and role membership; 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	NIST SP 800-53B R5 Baseline: Low	AC-2	AC-2	AC-2	AC-2

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)	Low	Mod	High	Privacy
AC-2	Account Management	a. Define and document the types of accounts allowed and specifically prohibited for use within the system;b. Assign account managers;c. Require [Assignment: organization-defined prerequisites and criteria] for group and role membership;d. Specify:1. Authorized users of the system;2. Group and role membership; 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	NIST SP 800-53B R5 Baseline: Low	AC-2	AC-2	AC-2	AC-2
AC-2	Account Management	a. Define and document the types of accounts allowed and specifically prohibited for use within the system;b. Assign account managers;c. Require [Assignment: organization-defined prerequisites and criteria] for group and role membership;d. Specify:1. Authorized users of the system;2. Group and role membership; 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	NIST SP 800-53B R5 Baseline: Low	AC-2	AC-2	AC-2	AC-2
AC-2(1)	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	NIST SP 800-53B R5 Baseline: Moderate		AC-2(1)	AC-2(1)	
AC-2(2)	Account Management | Automated Temporary and Emergency Account	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	10	NIST SP 800-53B R5 Baseline: Moderate		AC-2(2)	AC-2(2)	
AC-2(3)	Account Management | Disable Accounts	Disable accounts within [Assignment: organization-defined time period] when the accounts:a. Have expired;b. Are no longer associated with a user or individual;c. Are in violation of organizational policy; 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	NIST SP 800-53B R5 Baseline: Moderate		AC-2(3)	AC-2(3)	
AC-2(4)	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	NIST SP 800-53B R5 Baseline: Moderate		AC-2(4)	AC-2(4)	
AC-2(5)	Account Management | Inactivity Logout	Require that users log out when [Assignment: organization-defined time period of expected inactivity or description of when to log out].	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	10	NIST SP 800-53B R5 Baseline: Moderate		AC-2(5)	AC-2(5)	
AC-2(6)	Account Management | Dynamic Privilege Management	Implement [Assignment: organization-defined dynamic privilege management capabilities].	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
AC-2(7)	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 a Role-Based Access Control (RBAC) policy over users and resources that applies need-to-know and fine-grained access control for sensitive/regulated data access.	10	NIST SP 800-53B R5 Baseline: Not Selected				
AC-2(8)	Account Management | Dynamic Account Management	Create, activate, manage, and deactivate [Assignment: organization-defined system accounts] dynamically.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
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].	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	NIST SP 800-53B R5 Baseline: Not Selected				
AC-2(10)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
AC-2(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	NIST SP 800-53B R5 Baseline: High			AC-2(11)	
AC-2(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 detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	10	NIST SP 800-53B R5 Baseline: High			AC-2(12)	
AC-2(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 systems and applications upon termination, as determined by management.	5	NIST SP 800-53B R5 Baseline: Moderate	AC-2(13)	AC-2(13)	AC-2(13)	AC-2(13)
AC-2(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	NIST SP 800-53B R5 Baseline: Moderate	AC-2(13)	AC-2(13)	AC-2(13)	AC-2(13)
AC-3	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	NIST SP 800-53B R5 Baseline: Low	AC-3	AC-3	AC-3	AC-3
AC-3	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	NIST SP 800-53B R5 Baseline: Low	AC-3	AC-3	AC-3	AC-3

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)	Low	Mod	High	Privacy
AC-3	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	NIST SP 800-53B R5 Baseline: Low	AC-3	AC-3	AC-3	AC-3
AC-3(1)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
AC-3(2)	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 systems.	5	NIST SP 800-53B R5 Baseline: Not Selected	AC-3(2)	AC-3(2)	AC-3(2)	AC-3(2)
AC-3(2)	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	NIST SP 800-53B R5 Baseline: Not Selected	AC-3(2)	AC-3(2)	AC-3(2)	AC-3(2)
AC-3(3)	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	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
AC-3(4)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
AC-3(5)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
AC-3(6)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
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].	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
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].	Functional	Equal	Revocation of Access Authorizations	IAC-20.6	Mechanisms exist to revoke logical and physical access authorizations.	10	NIST SP 800-53B R5 Baseline: Not Selected				
AC-3(9)	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	Functional	Equal	Controlled Release	DCH-03.3	Automated mechanisms exist to validate cybersecurity & data privacy attributes prior to releasing information to external systems.	10	NIST SP 800-53B R5 Baseline: Not Selected				
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] by [Assignment: organization-defined roles].	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
AC-3(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 systems, applications and processes to restrict access to sensitive/regulated data.	10	NIST SP 800-53B R5 Baseline: Not Selected				
AC-3(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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
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	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
AC-3(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 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	NIST SP 800-53B R5 Baseline: Not Selected				AC-3(14)
AC-3(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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
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].	Functional	Equal	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.	10	NIST SP 800-53B R5 Baseline: Moderate		AC-4	AC-4	
AC-4(1)	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	10	NIST SP 800-53B R5 Baseline: Not Selected				
AC-4(2)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
AC-4(3)	Information Flow Enforcement | Dynamic Information Flow Control	Enforce [Assignment: organization-defined information flow control policies].	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: 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 (optional)	Notes (optional)	Low	Mod	High	Privacy
AC-4(4)	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	Functional	Equal	Content Check for Encrypted Data	NET-04.3	Mechanisms exist to prevent encrypted data from bypassing content-checking mechanisms.	10	NIST SP 800-53B R5 Baseline: High			AC-4(4)	
AC-4(5)	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	NIST SP 800-53B R5 Baseline: Not Selected				
AC-4(6)	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	NIST SP 800-53B R5 Baseline: Not Selected				
AC-4(7)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
AC-4(8)	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	NIST SP 800-53B R5 Baseline: Not Selected				
AC-4(9)	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	NIST SP 800-53B R5 Baseline: Not Selected				
AC-4(10)	Information Flow Enforcement | Enable and Disable Security or Privacy Policy	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
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 policies.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
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.	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	10	NIST SP 800-53B R5 Baseline: Not Selected				
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.	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	10	NIST SP 800-53B R5 Baseline: Not Selected				
AC-4(14)	Information Flow Enforcement | Security or Privacy Policy Filter	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
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 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	10	NIST SP 800-53B R5 Baseline: Not Selected				
AC-4(16)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
AC-4(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	NIST SP 800-53B R5 Baseline: Not Selected				
AC-4(18)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
AC-4(19)	Information Flow Enforcement | Validation of	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 privacy filters on metadata.	10	NIST SP 800-53B R5 Baseline: Not Selected				
AC-4(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	10	NIST SP 800-53B R5 Baseline: Not Selected				
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 required separations by types of information].	Functional	Equal	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate systems, applications and services that protections from other network resources.	10	NIST SP 800-53B R5 Baseline: Not Selected				
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 flow between the different security domains.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
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 action].	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
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 intended specification.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
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, 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	NIST SP 800-53B R5 Baseline: Not Selected				
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 filtered.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
AC-4(27)	Information Flow Enforcement | Redundant/independent Filtering	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
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.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
AC-4(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-	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
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.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: 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 (optional)	Notes (optional)	Low	Mod	High	Privacy
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.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
AC-4(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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
AC-5	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	NIST SP 800-53B R5 Baseline: Moderate	AC-5	AC-5	AC-5	AC-5
AC-5	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 assets.	5	NIST SP 800-53B R5 Baseline: Moderate	AC-5	AC-5	AC-5	AC-5
AC-5	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	NIST SP 800-53B R5 Baseline: Moderate	AC-5	AC-5	AC-5	AC-5
AC-5	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	NIST SP 800-53B R5 Baseline: Moderate	AC-5	AC-5	AC-5	AC-5
AC-6	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	NIST SP 800-53B R5 Baseline: Moderate	AC-6	AC-6	AC-6	AC-6
AC-6	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	NIST SP 800-53B R5 Baseline: Moderate	AC-6	AC-6	AC-6	AC-6
AC-6(1)	Least Privilege | Authorize Access to Security Functions	Authorize access for [Assignment: organization-defined individuals or roles] to:a. [Assignment: organization-defined security functions (deployed in hardware, software, and firmware)]; andb. [Assignment: organization-defined security-	Functional	Equal	Authorize Access to Security Functions	IAC-21.1	Mechanisms exist to limit access to security functions to explicitly-authorized privileged users.	10	NIST SP 800-53B R5 Baseline: Moderate		AC-6(1)	AC-6(1)	
AC-6(2)	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	NIST SP 800-53B R5 Baseline: Moderate		AC-6(2)	AC-6(2)	
AC-6(3)	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 systems or where sensitive/regulated data is stored, transmitted and/or processed only for compelling operational	10	NIST SP 800-53B R5 Baseline: High			AC-6(3)	
AC-6(4)	Least Privilege | Separate Processing Domains	Provide separate processing domains to enable finer-grained allocation of user privileges.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
AC-6(5)	Least Privilege | Privileged Accounts	Restrict privileged accounts on the system to [Assignment: organization-defined personnel or roles].	Functional	Equal	Privileged Accounts	IAC-21.3	Mechanisms exist to restrict the assignment of privileged accounts to organization-defined personnel or roles without management approval.	10	NIST SP 800-53B R5 Baseline: Moderate		AC-6(5)	AC-6(5)	
AC-6(6)	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	NIST SP 800-53B R5 Baseline: Not Selected				
AC-6(7)	Least Privilege | Review of User Privileges	a. Review [Assignment: organization-defined frequency] the privileges assigned to [Assignment: organization-defined roles or classes of users] to validate the need for such privileges; 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	NIST SP 800-53B R5 Baseline: Moderate		AC-6(7)	AC-6(7)	
AC-6(8)	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	NIST SP 800-53B R5 Baseline: Not Selected				
AC-6(9)	Least Privilege | Log Use of Privileged	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	NIST SP 800-53B R5 Baseline: Moderate		AC-6(9)	AC-6(9)	
AC-6(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 /	10	NIST SP 800-53B R5 Baseline: Moderate		AC-6(10)	AC-6(10)	
AC-7	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	NIST SP 800-53B R5 Baseline: Low	AC-7	AC-7	AC-7	
AC-7(1)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
AC-7(2)	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	NIST SP 800-53B R5 Baseline: Not Selected				
AC-7(3)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
AC-7(4)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: 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 (optional)	Notes (optional)	Low	Mod	High	Privacy
AC-8	System Use Notification	a. Display [Assignment: organization-defined system use notification message or banner] to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and state that:1. Users are accessing a U.S. Government system;2. System usage may be monitored, recorded, and subject to audit;3. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; 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	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 the system that provides cybersecurity & data privacy notices.	10	NIST SP 800-53B R5 Baseline: Low	AC-8	AC-8	AC-8	
AC-9	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	10	NIST SP 800-53B R5 Baseline: Not Selected				
AC-9(1)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
AC-9(2)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
AC-9(3)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
AC-9(4)	Previous Logon Notification | Additional Logon	Notify the user, upon successful logon, of the following additional information: [Assignment: organization-defined additional information].	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: 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	NIST SP 800-53B R5 Baseline: High			AC-10	
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	5	NIST SP 800-53B R5 Baseline: Moderate		AC-11	AC-11	
AC-11(1)	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	NIST SP 800-53B R5 Baseline: Moderate		AC-11(1)	AC-11(1)	
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	NIST SP 800-53B R5 Baseline: Moderate		AC-12	AC-12	
AC-12(1)	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	10	NIST SP 800-53B R5 Baseline: Not Selected				
AC-12(2)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
AC-12(3)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
AC-13	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	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	NIST SP 800-53B R5 Baseline: Low	AC-14	AC-14	AC-14	
AC-14(1)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
AC-15	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	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:	Functional	Equal	Cybersecurity & Data Privacy Attributes	DCH-05	Mechanisms exist to bind cybersecurity & data privacy attributes to information as it is stored, transmitted and processed.	10	NIST SP 800-53B R5 Baseline: Not Selected				
AC-16(1)	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 & data privacy attributes with individuals and objects as information is created, combined, or transformed, in accordance with organization-defined cybersecurity and data privacy	10	NIST SP 800-53B R5 Baseline: Not Selected				
AC-16(2)	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 & data privacy attributes.	10	NIST SP 800-53B R5 Baseline: Not Selected				
AC-16(3)	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 & data privacy attributes to individuals and objects.	10	NIST SP 800-53B R5 Baseline: Not Selected				
AC-16(4)	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 & data privacy attributes with individuals and objects by authorized individuals (or processes acting on behalf of individuals).	10	NIST SP 800-53B R5 Baseline: Not Selected				
AC-16(5)	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 & data privacy 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	10	NIST SP 800-53B R5 Baseline: 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 (optional)	Notes (optional)	Low	Mod	High	Privacy
AC-16(6)	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 & data privacy attributes with individuals and objects in accordance with cybersecurity and data privacy	10	NIST SP 800-53B R5 Baseline: Not Selected				
AC-16(7)	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 & data privacy attributes employed in access enforcement and flow enforcement decisions between distributed system components.	10	NIST SP 800-53B R5 Baseline: Not Selected				
AC-16(8)	Security and Privacy Attributes | Association Techniques and	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 & data privacy attributes to information.	10	NIST SP 800-53B R5 Baseline: Not Selected				
AC-16(9)	Security and 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	NIST SP 800-53B R5 Baseline: 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 & data privacy attributes available for association with subjects and objects.	10	NIST SP 800-53B R5 Baseline: 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	NIST SP 800-53B R5 Baseline: Low	AC-17	AC-17	AC-17	
AC-17(1)	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	NIST SP 800-53B R5 Baseline: Moderate		AC-17(1)	AC-17(1)	
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.	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	NIST SP 800-53B R5 Baseline: Moderate		AC-17(2)	AC-17(2)	
AC-17(3)	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	NIST SP 800-53B R5 Baseline: Moderate		AC-17(3)	AC-17(3)	
AC-17(4)	Remote Access | Privileged Commands and Access	a. Authorize the execution of privileged commands and access to security-relevant information via remote access only in a format that provides assessable evidence and for the following needs: [Assignment: organization-defined needs]; andb. Document the rationale for remote access in the security plan	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	NIST SP 800-53B R5 Baseline: Moderate		AC-17(4)	AC-17(4)	
AC-17(5)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
AC-17(6)	Remote Access | Protection of Mechanism	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	NIST SP 800-53B R5 Baseline: Not Selected				
AC-17(7)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
AC-17(8)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
AC-17(9)	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	10	NIST SP 800-53B R5 Baseline: 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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: 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	NIST SP 800-53B R5 Baseline: Low	AC-18	AC-18	AC-18	AC-18
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	NIST SP 800-53B R5 Baseline: Low	AC-18	AC-18	AC-18	AC-18
AC-18(1)	Wireless Access | Authentication and Encryption	Protect wireless access to the system using authentication of [Selection (one or more): users; devices] and encryption.	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 to connect; and (2) Encrypting transmitted data.	10	NIST SP 800-53B R5 Baseline: Moderate		AC-18(1)	AC-18(1)	
AC-18(2)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
AC-18(3)	Wireless Access | Disable Wireless Networking	Disable, when not intended for use, wireless networking capabilities embedded within system components prior to issuance and deployment.	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	10	NIST SP 800-53B R5 Baseline: Moderate		AC-18(3)	AC-18(3)	
AC-18(4)	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	NIST SP 800-53B R5 Baseline: High			AC-18(4)	
AC-18(5)	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	NIST SP 800-53B R5 Baseline: High			AC-18(5)	
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 systems.	10	NIST SP 800-53B R5 Baseline: Low	AC-19	AC-19	AC-19	
AC-19(1)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
AC-19(2)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
AC-19(3)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
AC-19(4)	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	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
AC-19(5)	Access Control for Mobile Devices | Full Device or Container-based Encryption	Employ [Selection: full-device encryption; container-based encryption] to protect the confidentiality and integrity of information on [Assignment: organization-defined mobile devices].	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	NIST SP 800-53B R5 Baseline: Moderate		AC-19(5)	AC-19(5)	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)	Low	Mod	High	Privacy
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	Functional	Equal	Use of External Information Systems	DCH-13	Mechanisms exist to govern how external parties, systems and services are used to securely store, process and transmit data.	10	NIST SP 800-53B R5 Baseline: Low	AC-20	AC-20	AC-20	
AC-20(1)	Use of External Systems | Limits on Authorized Use	Permit authorized individuals to use an external system to access the system or to process, store, or transmit organization-controlled information only after:a. Verification of the implementation of controls on the external system as specified in the organization’s security and privacy policies and security and privacy plans; 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, systems and services from storing, processing and transmitting data unless authorized individuals first: (1) Verifying the implementation of required security controls; or (2) Retaining a processing agreement with the entity hosting the external	10	NIST SP 800-53B R5 Baseline: Moderate		AC-20(1)	AC-20(1)	
AC-20(2)	Use of External Systems | Portable Storage Devices — Restricted Use	Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems using [Assignment: organization-defined restrictions].	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	NIST SP 800-53B R5 Baseline: Moderate		AC-20(2)	AC-20(2)	
AC-20(3)	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 Systems / Components / Devices	DCH-13.4	Mechanisms exist to restrict the use of non-organizationally owned information systems, system components or devices to process, store or transmit organizational	10	NIST SP 800-53B R5 Baseline: Not Selected				
AC-20(4)	Use of External Systems | Network Accessible Storage Devices — Prohibited	Prohibit the use of [Assignment: organization-defined network accessible storage devices] in external systems.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
AC-20(5)	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	NIST SP 800-53B R5 Baseline: 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	NIST SP 800-53B R5 Baseline: Moderate	AC-21	AC-21	AC-21	AC-21
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	NIST SP 800-53B R5 Baseline: Moderate	AC-21	AC-21	AC-21	AC-21
AC-21(1)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
AC-21(2)	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 information systems implement data search and retrieval functions that properly enforce data protection /	10	NIST SP 800-53B R5 Baseline: 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	NIST SP 800-53B R5 Baseline: Low	AC-22	AC-22	AC-22	
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	NIST SP 800-53B R5 Baseline: Not Selected	AC-23	AC-23	AC-23	AC-23
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, updating and/or sharing 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 (3) What is consistent with applicable laws, regulations and contractual obligations.	5	NIST SP 800-53B R5 Baseline: Not Selected	AC-23	AC-23	AC-23	AC-23
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	NIST SP 800-53B R5 Baseline: Not Selected				
AC-24(1)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
AC-24(2)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: 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	10	NIST SP 800-53B R5 Baseline: Not Selected				
AT-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] awareness and training policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 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	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	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 continuing suitability, adequacy and effectiveness.	5	NIST SP 800-53B R5 Baseline: Low	AT-1	AT-1	AT-1	AT-1

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)	Low	Mod	High	Privacy
AT-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] awareness and training policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 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	Functional	Subset Of	Cybersecurity & Data Privacy-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	NIST SP 800-53B R5 Baseline: Low	AT-1	AT-1	AT-1	AT-1
AT-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] awareness and training policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 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	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	NIST SP 800-53B R5 Baseline: Low	AT-1	AT-1	AT-1	AT-1
AT-2	Literacy Training and Awareness	a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors):1. As part of initial training for new users and [Assignment: organization-defined frequency] thereafter; 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	Cybersecurity & Data Privacy Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	10	NIST SP 800-53B R5 Baseline: Low	AT-2	AT-2	AT-2	AT-2
AT-2(1)	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	NIST SP 800-53B R5 Baseline: Not Selected				
AT-2(2)	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	NIST SP 800-53B R5 Baseline: Low	AT-2(2)	AT-2(2)	AT-2(2)	
AT-2(3)	Literacy Training and Awareness | Social Engineering and Mining	Provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining.	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	10	NIST SP 800-53B R5 Baseline: Moderate		AT-2(3)	AT-2(3)	
AT-2(4)	Literacy Training and Awareness | Suspicious Communications and Anomalous System	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	NIST SP 800-53B R5 Baseline: Not Selected				
AT-2(5)	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	NIST SP 800-53B R5 Baseline: Not Selected				
AT-2(6)	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 cybersecurity & data privacy awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.	10	NIST SP 800-53B R5 Baseline: Not Selected				
AT-3	Role-based Training	a. Provide role-based security and privacy training to personnel with the following roles and responsibilities: [Assignment: organization-defined roles and responsibilities]:1. Before authorizing access to the system, information, or performing assigned duties, and [Assignment: organization-defined frequency] thereafter; 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	Functional	Intersects With	Role-Based Cybersecurity & Data Privacy Training	SAT-03	Mechanisms exist to provide role-based cybersecurity & data privacy-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5	NIST SP 800-53B R5 Baseline: Low	AT-3	AT-3	AT-3	AT-3
AT-3(1)	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	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
AT-3(2)	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 Cybersecurity & Data Privacy Training	SAT-03	Mechanisms exist to provide role-based cybersecurity & data privacy-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and	5	NIST SP 800-53B R5 Baseline: Not Selected				
AT-3(3)	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 cybersecurity & data privacy training that reinforce training objectives.	10	NIST SP 800-53B R5 Baseline: Not Selected				
AT-3(4)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
AT-3(5)	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	10	NIST SP 800-53B R5 Baseline: Not Selected				AT-3(5)
AT-4	Training Records	a. Document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training; andb. Retain individual training records for [Assignment: organization-defined time period].	Functional	Equal	Cybersecurity & Data Privacy Training Records	SAT-04	Mechanisms exist to document, retain and monitor individual training activities, including basic cybersecurity & data privacy awareness training, ongoing awareness training and specific-	10	NIST SP 800-53B R5 Baseline: Low	AT-4	AT-4	AT-4	AT-4
AT-5	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
AT-6	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	NIST SP 800-53B R5 Baseline: 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 (optional)	Notes (optional)	Low	Mod	High	Privacy
AU-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] audit and accountability policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 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 Cybersecurity & Data Protection Program	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 continuing suitability, adequacy and effectiveness.	5	NIST SP 800-53B R5 Baseline: Low	AU-1	AU-1	AU-1	AU-1
AU-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] audit and accountability policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 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 Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	NIST SP 800-53B R5 Baseline: Low	AU-1	AU-1	AU-1	AU-1
AU-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] audit and accountability policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 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	NIST SP 800-53B R5 Baseline: Low	AU-1	AU-1	AU-1	AU-1
AU-2	Event Logging	a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging];b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;c. Specify the following event types for logging within the system: [Assignment: organization-defined event types (subset of the event types defined in AU-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:	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	NIST SP 800-53B R5 Baseline: Low	AU-2	AU-2	AU-2	AU-2
AU-2	Event Logging	a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging];b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;c. Specify the following event types for logging within the system: [Assignment: organization-defined event types (subset of the event types defined in AU-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:	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	NIST SP 800-53B R5 Baseline: Low	AU-2	AU-2	AU-2	AU-2
AU-2(1)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
AU-2(2)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
AU-2(3)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
AU-2(4)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
AU-3	Content of Audit Records	Ensure that audit records contain information that establishes the following:a. What type of event occurred;b. When the event occurred;c. Where the event occurred;d. Source of the event;e. Outcome of the event; 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 systems 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	10	NIST SP 800-53B R5 Baseline: Low	AU-3	AU-3	AU-3	
AU-3(1)	Content of Audit Records | Additional Audit Information	Generate audit records containing the following additional information: [Assignment: organization-defined additional information].	Functional	Intersects With	Sensitive Audit Information	MON-03.1	Mechanisms exist to protect sensitive/regulated data contained in log files.	5	NIST SP 800-53B R5 Baseline: Moderate		AU-3(1)	AU-3(1)	
AU-3(2)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
AU-3(3)	Content of Audit Records | Limit Personally Identifiable Information Elements	Limit personally identifiable information contained in audit records to the following elements identified in the privacy risk assessment: [Assignment: organization-defined elements].	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.	10	NIST SP 800-53B R5 Baseline: Not Selected				AU-3(3)
AU-4	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	NIST SP 800-53B R5 Baseline: Low	AU-4	AU-4	AU-4	
AU-4(1)	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	NIST SP 800-53B R5 Baseline: 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 (optional)	Notes (optional)	Low	Mod	High	Privacy
AU-5	Response to Audit Logging Process Failures	a. Alert [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period] in the event of an audit logging process failure; 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	NIST SP 800-53B R5 Baseline: Low	AU-5	AU-5	AU-5	
AU-5(1)	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	NIST SP 800-53B R5 Baseline: High			AU-5(1)	
AU-5(2)	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	NIST SP 800-53B R5 Baseline: High			AU-5(2)	
AU-5(3)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
AU-5(4)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
AU-5(5)	Response to Audit Logging Process Failures | Alternate Audit Logging	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	NIST SP 800-53B R5 Baseline: Not Selected				
AU-6	Audit Record Review, Analysis, and Reporting	a. Review and analyze system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity] and the potential impact of the inappropriate or unusual activity;b. Report findings to [Assignment: organization-defined personnel or roles]; 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	NIST SP 800-53B R5 Baseline: Low	AU-6	AU-6	AU-6	AU-6
AU-6	Audit Record Review, Analysis, and Reporting	a. Review and analyze system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity] and the potential impact of the inappropriate or unusual activity;b. Report findings to [Assignment: organization-defined personnel or roles]; 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	NIST SP 800-53B R5 Baseline: Low	AU-6	AU-6	AU-6	AU-6
AU-6(1)	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 Audit Information	MON-03.1	Mechanisms exist to protect sensitive/regulated data contained in log files.	5	NIST SP 800-53B R5 Baseline: Moderate		AU-6(1)	AU-6(1)	
AU-6(2)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
AU-6(3)	Audit Record Review, Analysis, and Reporting | Correlate Audit Record Repositories	Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.	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	5	NIST SP 800-53B R5 Baseline: Moderate		AU-6(3)	AU-6(3)	
AU-6(4)	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	NIST SP 800-53B R5 Baseline: Not Selected				
AU-6(5)	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	10	NIST SP 800-53B R5 Baseline: High			AU-6(5)	
AU-6(6)	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	NIST SP 800-53B R5 Baseline: High			AU-6(6)	
AU-6(7)	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 systems associated with the review, analysis and reporting of audit information.	10	NIST SP 800-53B R5 Baseline: Not Selected				
AU-6(8)	Audit Record Review, Analysis, and Reporting | Full Text Analysis of Privileged	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	NIST SP 800-53B R5 Baseline: Not Selected				
AU-6(9)	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	5	NIST SP 800-53B R5 Baseline: Not Selected				
AU-6(10)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
AU-7	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	NIST SP 800-53B R5 Baseline: Moderate		AU-7	AU-7	
AU-7(1)	Audit Record Reduction and Report Generation | Automatic Processing	Provide and implement the capability to process, sort, and search audit records for events of interest based on the following content: [Assignment: organization-defined fields within audit records].	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	NIST SP 800-53B R5 Baseline: Moderate		AU-7(1)	AU-7(1)	
AU-7(2)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
AU-8	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	NIST SP 800-53B R5 Baseline: Low	AU-8	AU-8	AU-8	AU-8
AU-8	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 systems to use an authoritative time source to generate time stamps for event logs.	5	NIST SP 800-53B R5 Baseline: Low	AU-8	AU-8	AU-8	AU-8
AU-8(1)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
AU-8(2)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
AU-9	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	NIST SP 800-53B R5 Baseline: Low	AU-9	AU-9	AU-9	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)	Low	Mod	High	Privacy
AU-9(1)	Protection of Audit Information | Hardware Write-once	Write audit trails to hardware-enforced, write-once media.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
AU-9(2)	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	NIST SP 800-53B R5 Baseline: High			AU-9(2)	
AU-9(3)	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	NIST SP 800-53B R5 Baseline: High			AU-9(3)	
AU-9(4)	Protection of Audit Information | Access by Subset of Privileged Users	Authorize access to management of audit logging functionality to only [Assignment: organization-defined subset of privileged users or roles].	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	NIST SP 800-53B R5 Baseline: Moderate		AU-9(4)	AU-9(4)	
AU-9(5)	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	NIST SP 800-53B R5 Baseline: Not Selected				
AU-9(6)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
AU-9(7)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: 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	NIST SP 800-53B R5 Baseline: High			AU-10	
AU-10(1)	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	NIST SP 800-53B R5 Baseline: Not Selected				
AU-10(2)	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	NIST SP 800-53B R5 Baseline: Not Selected				
AU-10(3)	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	NIST SP 800-53B R5 Baseline: Not Selected				
AU-10(4)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
AU-10(5)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	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	NIST SP 800-53B R5 Baseline: Low	AU-11	AU-11	AU-11	AU-11
AU-11(1)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: 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	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	NIST SP 800-53B R5 Baseline: Low	AU-12	AU-12	AU-12	
AU-12(1)	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	NIST SP 800-53B R5 Baseline: High			AU-12(1)	
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.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
AU-12(3)	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 information system components, based on specific event criteria within specified	10	NIST SP 800-53B R5 Baseline: High			AU-12(3)	
AU-12(4)	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	NIST SP 800-53B R5 Baseline: 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	Functional	Equal	Monitoring For Information Disclosure	MON-11	Mechanisms exist to monitor for evidence of unauthorized exfiltration or disclosure of non-public information.	10	NIST SP 800-53B R5 Baseline: Not Selected				
AU-13(1)	Monitoring for Information Disclosure | Use of	Monitor open-source information and information sites using [Assignment: organization-defined automated mechanisms].	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
AU-13(2)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
AU-13(3)	Monitoring for Information Disclosure | Unauthorized Replication of	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: 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	NIST SP 800-53B R5 Baseline: Not Selected				
AU-14(1)	Session Audit | System Start-up	Initiate session audits automatically at system start-up.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
AU-14(2)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
AU-14(3)	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	10	NIST SP 800-53B R5 Baseline: 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 (optional)	Notes (optional)	Low	Mod	High	Privacy
AU-15	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	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	NIST SP 800-53B R5 Baseline: Not Selected				
AU-16(1)	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	NIST SP 800-53B R5 Baseline: Not Selected				
AU-16(2)	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	NIST SP 800-53B R5 Baseline: Not Selected				
AU-16(3)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
CA-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] 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:	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of cybersecurity & data privacy assessment and authorization controls.	10	NIST SP 800-53B R5 Baseline: Low	CA-1	CA-1	CA-1	CA-1
CA-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] 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:	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	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 continuing suitability, adequacy and effectiveness.	5	NIST SP 800-53B R5 Baseline: Low	CA-1	CA-1	CA-1	CA-1
CA-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] 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:	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	NIST SP 800-53B R5 Baseline: Low	CA-1	CA-1	CA-1	CA-1
CA-2	Control Assessments	a. Select the appropriate assessor or assessment team for the type of assessment to be conducted;b. Develop a control assessment plan that describes the scope of the assessment including:1. Controls and control enhancements under assessment;2. Assessment procedures to be used to determine control effectiveness; 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-	Functional	Intersects With	Functional Review Of Cybersecurity & Data Protection Controls	CPL-03.2	Mechanisms exist to regularly review technology assets for adherence to the organization's cybersecurity & data protection policies and standards.	5	NIST SP 800-53B R5 Baseline: Low	CA-2	CA-2	CA-2	CA-2
CA-2	Control Assessments	a. Select the appropriate assessor or assessment team for the type of assessment to be conducted;b. Develop a control assessment plan that describes the scope of the assessment including:1. Controls and control enhancements under assessment;2. Assessment procedures to be used to determine control effectiveness; 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-	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 cybersecurity & data privacy controls.	5	NIST SP 800-53B R5 Baseline: Low	CA-2	CA-2	CA-2	CA-2

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)	Low	Mod	High	Privacy
CA-2	Control Assessments	a. Select the appropriate assessor or assessment team for the type of assessment to be conducted;b. Develop a control assessment plan that describes the scope of the assessment including:1. Controls and control enhancements under assessment;2. Assessment procedures to be used to determine control effectiveness; 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-	Functional	Intersects With	Cybersecurity & Data Privacy In Project Management	PRM-04	Mechanisms exist to assess cybersecurity & data privacy 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	NIST SP 800-53B R5 Baseline: Low	CA-2	CA-2	CA-2	CA-2
CA-2	Control Assessments	a. Select the appropriate assessor or assessment team for the type of assessment to be conducted;b. Develop a control assessment plan that describes the scope of the assessment including:1. Controls and control enhancements under assessment;2. Assessment procedures to be used to determine control effectiveness; 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-	Functional	Intersects With	Assessments	IAO-02	Mechanisms exist to formally assess the cybersecurity & data privacy controls in systems, applications and services 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	NIST SP 800-53B R5 Baseline: Low	CA-2	CA-2	CA-2	CA-2
CA-2	Control Assessments	a. Select the appropriate assessor or assessment team for the type of assessment to be conducted;b. Develop a control assessment plan that describes the scope of the assessment including:1. Controls and control enhancements under assessment;2. Assessment procedures to be used to determine control effectiveness; 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-	Functional	Intersects With	Cybersecurity & Data Protection Assessments	CPL-03	Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's cybersecurity & data protection policies, standards and other applicable requirements.	5	NIST SP 800-53B R5 Baseline: Low	CA-2	CA-2	CA-2	CA-2
CA-2(1)	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 cybersecurity & data privacy control assessments.	10	NIST SP 800-53B R5 Baseline: Moderate		CA-2(1)	CA-2(1)	
CA-2(2)	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	5	NIST SP 800-53B R5 Baseline: High			CA-2(2)	
CA-2(3)	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	Functional	Equal	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.	10	NIST SP 800-53B R5 Baseline: Not Selected				
CA-3	Information Exchange	a. Approve and manage the exchange of information between the system and other systems using [Selection (one or more): interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service level agreements; user agreements; nondisclosure agreements; [Assignment: organization-defined type of agreement]];b. Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated; andc. Review and update the agreements [Assignment: organization-	Functional	Intersects With	System Interconnections	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, the interface characteristics, cybersecurity & data privacy requirements and the nature of the information communicated.	5	NIST SP 800-53B R5 Baseline: Low	CA-3	CA-3	CA-3	
CA-3(1)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
CA-3(2)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
CA-3(3)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
CA-3(4)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
CA-3(5)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
CA-3(6)	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 systems transferring data between interconnecting systems have the requisite authorizations (e.g., write permissions or privileges) prior to	10	NIST SP 800-53B R5 Baseline: High			CA-3(6)	
CA-3(7)	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	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
CA-4	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
CA-5	Plan of Action and Milestones	a. Develop a plan of action and milestones for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; 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	Functional	Intersects With	Plan of Action & Milestones (POA&M)	IAO-05	Mechanisms exist to generate a Plan of Action and Milestones (POA&M), or similar risk register, 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.	5	NIST SP 800-53B R5 Baseline: Low	CA-5	CA-5	CA-5	CA-5
CA-5(1)	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	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.	10	NIST SP 800-53B R5 Baseline: 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 (optional)	Notes (optional)	Low	Mod	High	Privacy
CA-6	Authorization	a. Assign a senior official as the authorizing official for the system;b. Assign a senior official as the authorizing official for common controls available for inheritance by organizational systems;c. Ensure that the authorizing official for the system, before commencing operations:1. Accepts the use of common controls inherited by the system; 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 systems, projects and services are officially authorized prior to "go live" in a production environment.	10	NIST SP 800-53B R5 Baseline: Low	CA-6	CA-6	CA-6	CA-6
CA-6(1)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
CA-6(2)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
CA-7	Continuous Monitoring	Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes:a. Establishing the following system-level metrics to be monitored: [Assignment: organization-defined system-level metrics];b. Establishing [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessment of control effectiveness;c. Ongoing control assessments in accordance with the continuous monitoring strategy;d. Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy;e. Correlation and analysis of information generated by control assessments and monitoring;f. Response actions to address results of the analysis of control assessment and monitoring information; andg. Reporting the security and privacy status of the system to [Assignment: organization-defined personnel or roles]	Functional	Intersects With	Cybersecurity & Data Protection Controls Oversight	CPL-02	Mechanisms exist to provide a cybersecurity & data protection controls oversight function that reports to the organization's executive leadership.	5	NIST SP 800-53B R5 Baseline: Low	CA-7	CA-7	CA-7	CA-7
CA-7(1)	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 cybersecurity & data protection controls at planned intervals or when the system, service or project	5	NIST SP 800-53B R5 Baseline: Moderate	CA-7(1)	CA-7(1)	CA-7(1)	CA-7(1)
CA-7(1)	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	Cybersecurity & Data Protection Controls Oversight	CPL-02	Mechanisms exist to provide a cybersecurity & data protection controls oversight function that reports to the organization's	5	NIST SP 800-53B R5 Baseline: Moderate	CA-7(1)	CA-7(1)	CA-7(1)	CA-7(1)
CA-7(2)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
CA-7(3)	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	10	NIST SP 800-53B R5 Baseline: Not Selected				
CA-7(4)	Continuous Monitoring | Risk Monitoring	Ensure risk monitoring is an integral part of the continuous monitoring strategy that includes the following:a. Effectiveness monitoring;b. Compliance monitoring; 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 cybersecurity & data privacy controls, compliance and change	10	NIST SP 800-53B R5 Baseline: Low	CA-7(4)	CA-7(4)	CA-7(4)	CA-7(4)
CA-7(5)	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	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
CA-7(6)	Continuous Monitoring | Automation Support	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
CA-8	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 systems and web applications.	10	NIST SP 800-53B R5 Baseline: High			CA-8	
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.	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	NIST SP 800-53B R5 Baseline: High			CA-8(1)	
CA-8(2)	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 systems and applications in accordance with organization-defined rules of engagement.	10	NIST SP 800-53B R5 Baseline: Not Selected				
CA-8(3)	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	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
CA-9	Internal System Connections	a. Authorize internal connections of [Assignment: organization-defined system components or classes of components] to the system;b. Document, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated;c. Terminate internal system connections after [Assignment: organization-defined conditions]; andd. Review [Assignment: organization-defined frequency] the continued need for each internal	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	NIST SP 800-53B R5 Baseline: Low	CA-9	CA-9	CA-9	
CA-9(1)	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.	10	NIST SP 800-53B R5 Baseline: Not Selected				
CM-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] configuration management policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 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	NIST SP 800-53B R5 Baseline: Low	CM-1	CM-1	CM-1	CM-1

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)	Low	Mod	High	Privacy
CM-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] configuration management policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 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 Cybersecurity & Data Protection Program	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 continuing suitability, adequacy and effectiveness.	5	NIST SP 800-53B R5 Baseline: Low	CM-1	CM-1	CM-1	CM-1
CM-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] configuration management policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 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 Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	NIST SP 800-53B R5 Baseline: Low	CM-1	CM-1	CM-1	CM-1
CM-2	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	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	NIST SP 800-53B R5 Baseline: Low	CM-2	CM-2	CM-2	CM-2
CM-2	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	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	NIST SP 800-53B R5 Baseline: Low	CM-2	CM-2	CM-2	CM-2
CM-2(1)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
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].	Functional	Equal	Automated Central Management & Verification	CFG-02.2	Automated mechanisms exist to govern and report on baseline configurations of systems through Continuous Diagnostics and Mitigation (CDM), or similar	10	NIST SP 800-53B R5 Baseline: Moderate		CM-2(2)	CM-2(2)	
CM-2(3)	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	NIST SP 800-53B R5 Baseline: Moderate		CM-2(3)	CM-2(3)	
CM-2(4)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
CM-2(5)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
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.	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	NIST SP 800-53B R5 Baseline: Not Selected				
CM-2(7)	Baseline Configuration | Configure Systems and Components for High-risk Areas	a. Issue [Assignment: organization-defined systems or system components] with [Assignment: organization-defined configurations] to individuals traveling to locations that the organization deems to be of significant risk; andb. Apply the following controls to the systems or components when the individuals return from travel: [Assignment: organization-defined controls].	Functional	Equal	Configure Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems utilized in high-risk areas with more restrictive baseline configurations.	10	NIST SP 800-53B R5 Baseline: Moderate		CM-2(7)	CM-2(7)	
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; 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	Functional	Subset Of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	NIST SP 800-53B R5 Baseline: Moderate	CM-3	CM-3	CM-3	CM-3
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; 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	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	NIST SP 800-53B R5 Baseline: Moderate	CM-3	CM-3	CM-3	CM-3
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; andf. Notify [Assignment: organization-defined personnel] when approved	Functional	Equal	Prohibition Of Changes	CHG-02.1	Mechanisms exist to prohibit unauthorized changes, unless organization-approved change requests are received.	10	NIST SP 800-53B R5 Baseline: High			CM-3(1)	
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.	Functional	Intersects With	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.	5	NIST SP 800-53B R5 Baseline: Moderate	CM-3(2)	CM-3(2)	CM-3(2)	CM-3(2)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)	Low	Mod	High	Privacy
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.	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	NIST SP 800-53B R5 Baseline: Moderate	CM-3(2)	CM-3(2)	CM-3(2)	CM-3(2)
CM-3(3)	Configuration Change Control | Automated Change	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
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].	Functional	Equal	Cybersecurity & Data Privacy Representative for Asset Lifecycle	CHG-02.3	Mechanisms exist to include a cybersecurity and/or data privacy representative in the configuration change control review process.	10	NIST SP 800-53B R5 Baseline: Moderate		CM-3(4)	CM-3(4)	
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].	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	NIST SP 800-53B R5 Baseline: Not Selected				
CM-3(6)	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	NIST SP 800-53B R5 Baseline: High			CM-3(6)	
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.	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	NIST SP 800-53B R5 Baseline: Not Selected				
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].	Functional	Equal	Configuration Enforcement	CFG-06	Automated mechanisms exist to monitor, enforce and report on configurations for endpoint devices.	10	NIST SP 800-53B R5 Baseline: Not Selected				
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].	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	NIST SP 800-53B R5 Baseline: Not Selected				
CM-4	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	NIST SP 800-53B R5 Baseline: Low	CM-4	CM-4	CM-4	CM-4
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.	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	10	NIST SP 800-53B R5 Baseline: High			CM-4(1)	
CM-4(2)	Impact Analyses | Verification of Controls	After system changes, verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security and privacy requirements for the system.	Functional	Equal	Technical Verification	IAO-06	Mechanisms exist to perform Information Assurance Program (IAP) activities to evaluate the design, implementation and effectiveness of technical cybersecurity & data privacy controls.	10	NIST SP 800-53B R5 Baseline: Moderate		CM-4(2)	CM-4(2)	
CM-5	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	5	NIST SP 800-53B R5 Baseline: Low	CM-5	CM-5	CM-5	CM-5
CM-5	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	NIST SP 800-53B R5 Baseline: Low	CM-5	CM-5	CM-5	CM-5
CM-5(1)	Access Restrictions for Change | Automated Access Enforcement and	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	NIST SP 800-53B R5 Baseline: High			CM-5(1)	
CM-5(2)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
CM-5(3)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
CM-5(4)	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 assets.	10	NIST SP 800-53B R5 Baseline: Not Selected				
CM-5(5)	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	NIST SP 800-53B R5 Baseline: Not Selected				
CM-5(6)	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	NIST SP 800-53B R5 Baseline: Not Selected				
CM-5(7)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
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]; andd. Monitor and control changes to the configuration	Functional	Intersects With	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	NIST SP 800-53B R5 Baseline: Low	CM-6	CM-6	CM-6	CM-6
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]; andd. Monitor and control changes to the configuration	Functional	Intersects With	Approved Configuration Deviations	CFG-02.7	Mechanisms exist to document, assess risk and approve or deny deviations to standardized configurations.	5	NIST SP 800-53B R5 Baseline: Low	CM-6	CM-6	CM-6	CM-6
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].	Functional	Intersects With	Automated Central Management & Verification	CFG-02.2	Automated mechanisms exist to govern and report on baseline configurations of systems through Continuous Diagnostics and Mitigation (CDM), or similar	5	NIST SP 800-53B R5 Baseline: High			CM-6(1)	
CM-6(2)	Configuration Settings | Respond to Unauthorized	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	10	NIST SP 800-53B R5 Baseline: High			CM-6(2)	
CM-6(3)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
CM-6(4)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
CM-7	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	NIST SP 800-53B R5 Baseline: Low	CM-7	CM-7	CM-7	
CM-7(1)	Least Functionality | Periodic Review	a. Review the system [Assignment: organization-defined frequency] to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services; 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	NIST SP 800-53B R5 Baseline: Moderate		CM-7(1)	CM-7(1)	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)	Low	Mod	High	Privacy
CM-7(2)	Least Functionality | Prevent Program Execution	Prevent program execution in accordance with [Selection (one or more): [Assignment: organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions]; rules authorizing the terms and conditions of software program usage].	Functional	Intersects With	Prevent Program Execution	SEA-06	Automated mechanisms exist to prevent the execution of unauthorized software programs.	5	NIST SP 800-53B R5 Baseline: Moderate	CM-7(2)	CM-7(2)	CM-7(2)	CM-7(2)
CM-7(2)	Least Functionality | Prevent Program Execution	Prevent program execution in accordance with [Selection (one or more): [Assignment: organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions]; rules authorizing the terms and conditions of software program usage].	Functional	Intersects With	Prevent Unauthorized Software Execution	CFG-03.2	Mechanisms exist to configure systems to prevent the execution of unauthorized software programs.	5	NIST SP 800-53B R5 Baseline: Moderate	CM-7(2)	CM-7(2)	CM-7(2)	CM-7(2)
CM-7(3)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
CM-7(4)	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	NIST SP 800-53B R5 Baseline: Not Selected				
CM-7(5)	Least Functionality | Authorized Software — Allow-by-exception	a. Identify [Assignment: organization-defined software programs authorized to execute on the system];b. Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system; 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	NIST SP 800-53B R5 Baseline: Moderate		CM-7(5)	CM-7(5)	
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].	Functional	Intersects With	Configure Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems utilized in high-risk areas with more restrictive baseline configurations.	5	NIST SP 800-53B R5 Baseline: Not Selected				
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:a. Obtained from sources with limited or no warranty; and/orb. Without the	Functional	Intersects With	Configure Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems utilized in high-risk areas with more restrictive baseline configurations.	5	NIST SP 800-53B R5 Baseline: Not Selected				
CM-7(8)	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	NIST SP 800-53B R5 Baseline: Not Selected				
CM-7(9)	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 Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems utilized in high-risk areas with more restrictive baseline configurations.	5	NIST SP 800-53B R5 Baseline: Not Selected				
CM-8	System Component Inventory	a. Develop and document an inventory of system components that:1. Accurately reflects the system;2. Includes all components within the system;3. Does not include duplicate accounting of components or components assigned to any other system;4. Is at the level of granularity deemed necessary for tracking and reporting; 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 that: (1) Accurately reflects the current systems, applications and services 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	5	NIST SP 800-53B R5 Baseline: Low	CM-8	CM-8	CM-8	CM-8
CM-8	System Component Inventory	a. Develop and document an inventory of system components that:1. Accurately reflects the system;2. Includes all components within the system;3. Does not include duplicate accounting of components or components assigned to any other system;4. Is at the level of granularity deemed necessary for tracking and reporting; 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	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	NIST SP 800-53B R5 Baseline: Low	CM-8	CM-8	CM-8	CM-8
CM-8(1)	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	NIST SP 800-53B R5 Baseline: Moderate		CM-8(1)	CM-8(1)	
CM-8(2)	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	10	NIST SP 800-53B R5 Baseline: High			CM-8(2)	
CM-8(3)	System Component Inventory | Automated Unauthorized Component Detection	a. Detect the presence of unauthorized hardware, software, and firmware components within the system using [Assignment: organization-defined automated mechanisms] [Assignment: organization-defined frequency]; 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	NIST SP 800-53B R5 Baseline: Moderate	CM-8(3)	CM-8(3)	CM-8(3)	CM-8(3)
CM-8(3)	System Component Inventory | Automated Unauthorized Component Detection	a. Detect the presence of unauthorized hardware, software, and firmware components within the system using [Assignment: organization-defined automated mechanisms] [Assignment: organization-defined frequency]; 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	NIST SP 800-53B R5 Baseline: Moderate	CM-8(3)	CM-8(3)	CM-8(3)	CM-8(3)
CM-8(3)	System Component Inventory | Automated Unauthorized Component Detection	a. Detect the presence of unauthorized hardware, software, and firmware components within the system using [Assignment: organization-defined automated mechanisms] [Assignment: organization-defined frequency]; 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	NIST SP 800-53B R5 Baseline: Moderate	CM-8(3)	CM-8(3)	CM-8(3)	CM-8(3)
CM-8(4)	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	10	NIST SP 800-53B R5 Baseline: High			CM-8(4)	
CM-8(5)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
CM-8(6)	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	NIST SP 800-53B R5 Baseline: Not Selected				
CM-8(7)	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	5	NIST SP 800-53B R5 Baseline: Not Selected				
CM-8(8)	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	NIST SP 800-53B R5 Baseline: 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 (optional)	Notes (optional)	Low	Mod	High	Privacy
CM-8(9)	System Component Inventory | Assignment of Components to	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	NIST SP 800-53B R5 Baseline: Not Selected				
CM-9	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	Functional	Subset Of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	NIST SP 800-53B R5 Baseline: Moderate	CM-9	CM-9	CM-9	CM-9
CM-9	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	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	NIST SP 800-53B R5 Baseline: Moderate	CM-9	CM-9	CM-9	CM-9
CM-9(1)	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	10	NIST SP 800-53B R5 Baseline: 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	Functional	Equal	Software Usage Restrictions	CFG-04	Mechanisms exist to enforce software usage restrictions to comply with applicable contract agreements and copyright laws.	10	NIST SP 800-53B R5 Baseline: Low	CM-10	CM-10	CM-10	
CM-10(1)	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	NIST SP 800-53B R5 Baseline: 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	Functional	Intersects With	Prohibit Installation Without Privileged Status	END-03	Automated mechanisms exist to prohibit software installations without explicitly assigned privileged status.	5	NIST SP 800-53B R5 Baseline: Low	CM-11	CM-11	CM-11	CM-11
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	Functional	Intersects With	User-Installed Software	CFG-05	Mechanisms exist to restrict the ability of non-privileged users to install unauthorized software.	5	NIST SP 800-53B R5 Baseline: Low	CM-11	CM-11	CM-11	CM-11
CM-11(1)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
CM-11(2)	User-installed Software | Software Installation with	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	NIST SP 800-53B R5 Baseline: Not Selected	CM-11(2)	CM-11(2)	CM-11(2)	CM-11(2)
CM-11(2)	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	5	NIST SP 800-53B R5 Baseline: Not Selected	CM-11(2)	CM-11(2)	CM-11(2)	CM-11(2)
CM-11(2)	User-installed Software | Software Installation with	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	5	NIST SP 800-53B R5 Baseline: Not Selected	CM-11(2)	CM-11(2)	CM-11(2)	CM-11(2)
CM-11(3)	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	NIST SP 800-53B R5 Baseline: Not Selected	CM-11(3)	CM-11(3)	CM-11(3)	CM-11(3)
CM-11(3)	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	NIST SP 800-53B R5 Baseline: Not Selected				
CM-11(3)	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	NIST SP 800-53B R5 Baseline: Not Selected	CM-11(3)	CM-11(3)	CM-11(3)	CM-11(3)
CM-11(3)	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	NIST SP 800-53B R5 Baseline: Not Selected	CM-11(3)	CM-11(3)	CM-11(3)	CM-11(3)
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	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	NIST SP 800-53B R5 Baseline: Moderate		CM-12	CM-12	
CM-12(1)	Information Location | Automated Tools to Support Information Location	Use automated tools to identify [Assignment: organization-defined information by information type] on [Assignment: organization-defined system components] to ensure controls are in place to protect organizational information and individual privacy.	Functional	Equal	Automated Tools to Support Information Location	DCH-24.1	Automated mechanisms exist to identify by data classification type to ensure adequate cybersecurity & data privacy controls are in place to protect organizational information and individual data privacy.	10	NIST SP 800-53B R5 Baseline: Moderate		CM-12(1)	CM-12(1)	
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 where sensitive/regulated data is stored, transmitted or processed.	10	NIST SP 800-53B R5 Baseline: 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	NIST SP 800-53B R5 Baseline: Not Selected				
CP-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] contingency planning policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 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:	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	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 continuing suitability, adequacy and effectiveness.	5	NIST SP 800-53B R5 Baseline: Low	CP-1	CP-1	CP-1	CP-1

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)	Low	Mod	High	Privacy
CP-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] contingency planning policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 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:	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	NIST SP 800-53B R5 Baseline: Low	CP-1	CP-1	CP-1	CP-1
CP-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] contingency planning policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 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:	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	NIST SP 800-53B R5 Baseline: Low	CP-1	CP-1	CP-1	CP-1
CP-2	Contingency Plan	a. Develop a contingency plan for the system that:1. Identifies essential mission and business functions and associated contingency requirements;2. Provides recovery objectives, restoration priorities, and metrics;3. Addresses contingency roles, responsibilities, assigned individuals with contact information;4. Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure;5. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented;6. Addresses the sharing of contingency information; 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;	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	NIST SP 800-53B R5 Baseline: Low	CP-2	CP-2	CP-2	CP-2
CP-2	Contingency Plan	a. Develop a contingency plan for the system that:1. Identifies essential mission and business functions and associated contingency requirements;2. Provides recovery objectives, restoration priorities, and metrics;3. Addresses contingency roles, responsibilities, assigned individuals with contact information;4. Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure;5. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented;6. Addresses the sharing of contingency information; 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;	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	NIST SP 800-53B R5 Baseline: Low	CP-2	CP-2	CP-2	CP-2
CP-2(1)	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	NIST SP 800-53B R5 Baseline: Moderate		CP-2(1)	CP-2(1)	
CP-2(2)	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	NIST SP 800-53B R5 Baseline: High			CP-2(2)	
CP-2(3)	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	5	NIST SP 800-53B R5 Baseline: Moderate	CP-2(3)	CP-2(3)	CP-2(3)	CP-2(3)
CP-2(3)	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	5	NIST SP 800-53B R5 Baseline: Moderate	CP-2(3)	CP-2(3)	CP-2(3)	CP-2(3)
CP-2(4)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
CP-2(5)	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	10	NIST SP 800-53B R5 Baseline: High			CP-2(5)	
CP-2(6)	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	NIST SP 800-53B R5 Baseline: Not Selected				
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 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	NIST SP 800-53B R5 Baseline: 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 (optional)	Notes (optional)	Low	Mod	High	Privacy
CP-2(8)	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 systems, applications and services that support essential missions and business functions.	10	NIST SP 800-53B R5 Baseline: Moderate		CP-2(8)	CP-2(8)	
CP-3	Contingency Training	a. Provide contingency training to system users consistent with assigned roles and responsibilities:1. Within [Assignment: organization-defined time period] of assuming a contingency role or responsibility;2. When required by system changes; 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	NIST SP 800-53B R5 Baseline: Low	CP-3	CP-3	CP-3	
CP-3(1)	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	10	NIST SP 800-53B R5 Baseline: High			CP-3(1)	
CP-3(2)	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	NIST SP 800-53B R5 Baseline: Not Selected				
CP-4	Contingency Plan Testing	a. Test the contingency plan for the system [Assignment: organization-defined frequency] using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: [Assignment: organization-defined tests].b. Review the contingency plan test results; 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	NIST SP 800-53B R5 Baseline: Low	CP-4	CP-4	CP-4	CP-4
CP-4	Contingency Plan Testing	a. Test the contingency plan for the system [Assignment: organization-defined frequency] using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: [Assignment: organization-defined tests].b. Review the contingency plan test results; 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	NIST SP 800-53B R5 Baseline: Low	CP-4	CP-4	CP-4	CP-4
CP-4(1)	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	NIST SP 800-53B R5 Baseline: Moderate		CP-4(1)	CP-4(1)	
CP-4(2)	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	NIST SP 800-53B R5 Baseline: High			CP-4(2)	
CP-4(3)	Contingency Plan Testing | Automated Testing	Test the contingency plan using [Assignment: organization-defined automated mechanisms].	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
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.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
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 or	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
CP-5	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
CP-6	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	10	NIST SP 800-53B R5 Baseline: Moderate		CP-6	CP-6	
CP-6(1)	Alternate Storage Site | Separation from Primary Site	Identify an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats.	Functional	Equal	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.	10	NIST SP 800-53B R5 Baseline: Moderate		CP-6(1)	CP-6(1)	
CP-6(2)	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	5	NIST SP 800-53B R5 Baseline: High			CP-6(2)	
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 disaster and outline explicit mitigation actions.	Functional	Equal	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.	10	NIST SP 800-53B R5 Baseline: Moderate		CP-6(3)	CP-6(3)	
CP-7	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	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	NIST SP 800-53B R5 Baseline: Moderate		CP-7	CP-7	
CP-7(1)	Alternate Processing Site | Separation from Primary Site	Identify an alternate processing site that is sufficiently separated from the primary processing site to reduce susceptibility to the same threats.	Functional	Equal	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.	10	NIST SP 800-53B R5 Baseline: Moderate		CP-7(1)	CP-7(1)	
CP-7(2)	Alternate Processing Site | Accessibility	Identify potential accessibility problems to alternate processing sites in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.	Functional	Equal	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.	10	NIST SP 800-53B R5 Baseline: Moderate		CP-7(2)	CP-7(2)	
CP-7(3)	Alternate Processing Site | Priority of Service	Develop alternate processing site agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives).	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	NIST SP 800-53B R5 Baseline: Moderate		CP-7(3)	CP-7(3)	
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 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	NIST SP 800-53B R5 Baseline: High			CP-7(4)	
CP-7(5)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
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.	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	10	NIST SP 800-53B R5 Baseline: Not Selected				
CP-8	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	NIST SP 800-53B R5 Baseline: Moderate		CP-8	CP-8	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)	Low	Mod	High	Privacy
CP-8(1)	Telecommunications Services | Priority of Service Provisions	a. Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives); 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	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	NIST SP 800-53B R5 Baseline: Moderate		CP-8(1)	CP-8(1)	
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 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	5	NIST SP 800-53B R5 Baseline: Moderate		CP-8(2)	CP-8(2)	
CP-8(3)	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	NIST SP 800-53B R5 Baseline: High			CP-8(3)	
CP-8(4)	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	NIST SP 800-53B R5 Baseline: High			CP-8(4)	
CP-8(5)	Telecommunications Services | Alternate Telecommunication Service Testing	Test alternate telecommunication services [Assignment: organization-defined frequency].	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
CP-9	System Backup	a. Conduct backups of user-level information contained in [Assignment: organization-defined system components] [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives];b. Conduct backups of system-level information contained in the system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives];c. Conduct backups of system documentation, including security- and privacy-related documentation [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; 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 satisfying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	NIST SP 800-53B R5 Baseline: Low	CP-9	CP-9	CP-9	
CP-9(1)	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	NIST SP 800-53B R5 Baseline: Moderate		CP-9(1)	CP-9(1)	
CP-9(2)	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	NIST SP 800-53B R5 Baseline: High			CP-9(2)	
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 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	NIST SP 800-53B R5 Baseline: High			CP-9(3)	
CP-9(4)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
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 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	NIST SP 800-53B R5 Baseline: High			CP-9(5)	
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 information or disruption to operations.	Functional	Equal	Redundant Secondary System	BCD-11.7	Mechanisms exist to maintain a failover system, which is not collocated with the primary system, application and/or service, which can be activated with little-to-no loss of information or disruption to	10	NIST SP 800-53B R5 Baseline: Not Selected				
CP-9(7)	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	NIST SP 800-53B R5 Baseline: Not Selected				
CP-9(8)	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	NIST SP 800-53B R5 Baseline: Moderate		CP-9(8)	CP-9(8)	
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	Information System Recovery & Reconstitution	BCD-12	Mechanisms exist to ensure the secure recovery and reconstitution of systems to a known state after a disruption, compromise or failure.	5	NIST SP 800-53B R5 Baseline: Low	CP-10	CP-10	CP-10	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 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 assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	5	NIST SP 800-53B R5 Baseline: Low	CP-10	CP-10	CP-10	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 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	5	NIST SP 800-53B R5 Baseline: Low	CP-10	CP-10	CP-10	CP-10
CP-10(1)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
CP-10(2)	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 applications and services in accordance with Recovery Point Objectives (RPOs).	10	NIST SP 800-53B R5 Baseline: Moderate		CP-10(2)	CP-10(2)	
CP-10(3)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
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 information representing a known, operational state for the components.	Functional	Equal	Restore Within Time Period	BCD-12.4	Mechanisms exist to restore systems, applications and/or services within organization-defined restoration time-periods from configuration-controlled and integrity-protected information; representing a known, operational state for the asset.	10	NIST SP 800-53B R5 Baseline: High			CP-10(4)	
CP-10(5)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
CP-10(6)	System Recovery and Reconstitution | Component	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	NIST SP 800-53B R5 Baseline: 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	5	NIST SP 800-53B R5 Baseline: 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 enable systems to fail to an organization-defined known-state for types of failures, preserving system state information	5	NIST SP 800-53B R5 Baseline: 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	NIST SP 800-53B R5 Baseline: 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 (optional)	Notes (optional)	Low	Mod	High	Privacy
IA-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] identification and authentication policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 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:	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	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 continuing suitability, adequacy and effectiveness.	5	NIST SP 800-53B R5 Baseline: Low	IA-1	IA-1	IA-1	IA-1
IA-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] identification and authentication policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 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:	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	NIST SP 800-53B R5 Baseline: Low	IA-1	IA-1	IA-1	IA-1
IA-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] identification and authentication policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 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:	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	NIST SP 800-53B R5 Baseline: Low	IA-1	IA-1	IA-1	IA-1
IA-2	Identification and Authentication (organizational Users)	Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.	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	NIST SP 800-53B R5 Baseline: Low	IA-2	IA-2	IA-2	
IA-2(1)	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 systems, applications and/or services; and/ or (3) Non-console access to critical systems or systems that store, transmit and/or process	5	NIST SP 800-53B R5 Baseline: Low	IA-2(1)	IA-2(1)	IA-2(1)	IA-2(1)
IA-2(1)	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	NIST SP 800-53B R5 Baseline: Low	IA-2(1)	IA-2(1)	IA-2(1)	IA-2(1)
IA-2(1)	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-	5	NIST SP 800-53B R5 Baseline: Low	IA-2(1)	IA-2(1)	IA-2(1)	IA-2(1)
IA-2(1)	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	NIST SP 800-53B R5 Baseline: Low	IA-2(1)	IA-2(1)	IA-2(1)	IA-2(1)
IA-2(1)	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	NIST SP 800-53B R5 Baseline: Low	IA-2(1)	IA-2(1)	IA-2(1)	IA-2(1)
IA-2(1)	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	NIST SP 800-53B R5 Baseline: Low	IA-2(1)	IA-2(1)	IA-2(1)	IA-2(1)
IA-2(1)	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	NIST SP 800-53B R5 Baseline: Low	IA-2(1)	IA-2(1)	IA-2(1)	IA-2(1)
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.	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-	5	NIST SP 800-53B R5 Baseline: Low	IA-2(2)	IA-2(2)	IA-2(2)	IA-2(2)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)	Low	Mod	High	Privacy
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.	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	NIST SP 800-53B R5 Baseline: Low	IA-2(2)	IA-2(2)	IA-2(2)	IA-2(2)
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.	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	NIST SP 800-53B R5 Baseline: Low	IA-2(2)	IA-2(2)	IA-2(2)	IA-2(2)
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.	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	NIST SP 800-53B R5 Baseline: Low	IA-2(2)	IA-2(2)	IA-2(2)	IA-2(2)
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.	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	NIST SP 800-53B R5 Baseline: Low	IA-2(2)	IA-2(2)	IA-2(2)	IA-2(2)
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.	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 systems, applications and/or services; and/ or (3) Non-console access to critical systems or systems that store, transmit and/or process	5	NIST SP 800-53B R5 Baseline: Low	IA-2(2)	IA-2(2)	IA-2(2)	IA-2(2)
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.	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	NIST SP 800-53B R5 Baseline: Low	IA-2(2)	IA-2(2)	IA-2(2)	IA-2(2)
IA-2(3)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
IA-2(4)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
IA-2(5)	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	NIST SP 800-53B R5 Baseline: High			IA-2(5)	
IA-2(6)	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	NIST SP 800-53B R5 Baseline: Not Selected				
IA-2(7)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
IA-2(8)	Identification and Authentication (organizational Users) | Access to Accounts — Replay Resistant	Implement replay-resistant authentication mechanisms for access to [Selection (one or more): privileged accounts; non-privileged accounts].	Functional	Equal	Replay-Resistant Authentication	IAC-02.2	Automated mechanisms exist to employ replay-resistant authentication.	10	NIST SP 800-53B R5 Baseline: Low	IA-2(8)	IA-2(8)	IA-2(8)	
IA-2(9)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
IA-2(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 Single Sign-On (SSO) Transparent Authentication capability to the organization's systems and services.	10	NIST SP 800-53B R5 Baseline: Not Selected				
IA-2(11)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
IA-2(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	NIST SP 800-53B R5 Baseline: Low	IA-2(12)	IA-2(12)	IA-2(12)	
IA-2(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	NIST SP 800-53B R5 Baseline: Not Selected				
IA-3	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	NIST SP 800-53B R5 Baseline: Moderate		IA-3	IA-3	
IA-3(1)	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	NIST SP 800-53B R5 Baseline: Not Selected				
IA-3(2)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
IA-3(3)	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	NIST SP 800-53B R5 Baseline: Not Selected				
IA-3(4)	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	NIST SP 800-53B R5 Baseline: Not Selected	IA-3(4)	IA-3(4)	IA-3(4)	IA-3(4)
IA-3(4)	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	NIST SP 800-53B R5 Baseline: Not Selected	IA-3(4)	IA-3(4)	IA-3(4)	IA-3(4)
IA-4	Identifier Management	Manage system identifiers by:a. Receiving authorization from [Assignment: organization-defined personnel or roles] to assign an individual, group, role, service, or device identifier;b. Selecting an identifier that identifies an individual, group, role, service, or device;c. Assigning the identifier to the intended individual, group, role, service, or device; andd. Preventing reuse of identifiers for [Assignment: organization-defined time	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	NIST SP 800-53B R5 Baseline: Low	IA-4	IA-4	IA-4	IA-4

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)	Low	Mod	High	Privacy
IA-4	Identifier Management	Manage system identifiers by:a. Receiving authorization from [Assignment: organization-defined personnel or roles] to assign an individual, group, role, service, or device identifier;b. Selecting an identifier that identifies an individual, group, role, service, or device;c. Assigning the identifier to the intended individual, group, role, service, or device; andd. Preventing reuse of identifiers for [Assignment: organization-defined time	Functional	Intersects With	Identifier Management (User Names)	IAC-09	Mechanisms exist to govern naming standards for usernames and systems.	5	NIST SP 800-53B R5 Baseline: Low	IA-4	IA-4	IA-4	IA-4
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.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
IA-4(2)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
IA-4(3)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
IA-4(4)	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	NIST SP 800-53B R5 Baseline: Moderate	IA-4(4)	IA-4(4)	IA-4(4)	IA-4(4)
IA-4(4)	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	5	NIST SP 800-53B R5 Baseline: Moderate	IA-4(4)	IA-4(4)	IA-4(4)	IA-4(4)
IA-4(4)	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	NIST SP 800-53B R5 Baseline: Moderate	IA-4(4)	IA-4(4)	IA-4(4)	IA-4(4)
IA-4(5)	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	NIST SP 800-53B R5 Baseline: Not Selected				
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].	Functional	Equal	Cross-Organization Management	IAC-09.4	Mechanisms exist to coordinate username identifiers with external organizations for cross-organization management of identifiers.	10	NIST SP 800-53B R5 Baseline: Not Selected				
IA-4(7)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
IA-4(8)	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	10	NIST SP 800-53B R5 Baseline: Not Selected				
IA-4(9)	Identifier 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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
IA-5	Authenticator Management	Manage system authenticators by:a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator;b. Establishing initial authenticator content for any authenticators issued by the organization;c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators;e. Changing default authenticators prior to first use;f. Changing or refreshing authenticators [Assignment: organization-defined time period by authenticator type] or when [Assignment: organization-defined events] occur;g. Protecting authenticator content from unauthorized disclosure and modification;h. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; andi. Changing authenticators for group or role accounts when	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	NIST SP 800-53B R5 Baseline: Low	IA-5	IA-5	IA-5	IA-5
IA-5	Authenticator Management	Manage system authenticators by:a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator;b. Establishing initial authenticator content for any authenticators issued by the organization;c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators;e. Changing default authenticators prior to first use;f. Changing or refreshing authenticators [Assignment: organization-defined time period by authenticator type] or when [Assignment: organization-defined events] occur;g. Protecting authenticator content from unauthorized disclosure and modification;h. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; 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	NIST SP 800-53B R5 Baseline: Low	IA-5	IA-5	IA-5	IA-5
IA-5(1)	Authenticator Management | Password-based Authentication	For password-based authentication:a. Maintain a list of commonly-used, expected, or compromised passwords and update the list [Assignment: organization-defined frequency] and when organizational passwords are suspected to have been compromised directly or indirectly;b. Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5(1)(a);c. Transmit passwords only over cryptographically-protected channels;d. Store passwords using an approved salted key derivation function, preferably using a keyed hash;e. Require immediate selection of a new password upon account recovery;f. Allow user selection of long passwords and passphrases, including spaces and all printable characters;g. Employ automated tools to assist the user in selecting strong password authenticators; andh. Enforce the following composition and complexity rules: [Assignment: organization-defined composition and complexity	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	NIST SP 800-53B R5 Baseline: Low	IA-5(1)	IA-5(1)	IA-5(1)	IA-5(1)
IA-5(1)	Authenticator Management | Password-based Authentication	For password-based authentication:a. Maintain a list of commonly-used, expected, or compromised passwords and update the list [Assignment: organization-defined frequency] and when organizational passwords are suspected to have been compromised directly or indirectly;b. Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5(1)(a);c. Transmit passwords only over cryptographically-protected channels;d. Store passwords using an approved salted key derivation function, preferably using a keyed hash;e. Require immediate selection of a new password upon account recovery;f. Allow user selection of long passwords and passphrases, including spaces and all printable characters;g. Employ automated tools to assist the user in selecting strong password authenticators; andh. Enforce the following composition and complexity rules: [Assignment: organization-defined composition and complexity	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	NIST SP 800-53B R5 Baseline: Low	IA-5(1)	IA-5(1)	IA-5(1)	IA-5(1)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)	Low	Mod	High	Privacy
IA-5(1)	Authenticator Management | Password-based Authentication	For password-based authentication:a. Maintain a list of commonly-used, expected, or compromised passwords and update the list [Assignment: organization-defined frequency] and when organizational passwords are suspected to have been compromised directly or indirectly;b. Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5(1)(a);c. Transmit passwords only over cryptographically-protected channels;d. Store passwords using an approved salted key derivation function, preferably using a keyed hash;e. Require immediate selection of a new password upon account recovery;f. Allow user selection of long passwords and passphrases, including spaces and all printable characters;g. Employ automated tools to assist the user in selecting strong password authenticators; andh. Enforce the following composition and complexity rules: [Assignment: organization-defined composition and complexity	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	NIST SP 800-53B R5 Baseline: Low	IA-5(1)	IA-5(1)	IA-5(1)	IA-5(1)
IA-5(2)	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	NIST SP 800-53B R5 Baseline: Moderate	IA-5(2)	IA-5(2)	IA-5(2)	IA-5(2)
IA-5(3)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
IA-5(4)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
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.	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	NIST SP 800-53B R5 Baseline: Not Selected				
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.	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	NIST SP 800-53B R5 Baseline: Moderate	IA-5(6)	IA-5(6)	IA-5(6)	IA-5(6)
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.	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	NIST SP 800-53B R5 Baseline: Moderate	IA-5(6)	IA-5(6)	IA-5(6)	IA-5(6)
IA-5(7)	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	NIST SP 800-53B R5 Baseline: Not Selected				
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.	Functional	Intersects With	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 information systems.	5	NIST SP 800-53B R5 Baseline: Not Selected	IA-5(8)	IA-5(8)	IA-5(8)	IA-5(8)
IA-5(8)	Authenticator Management | Multiple System	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	5	NIST SP 800-53B R5 Baseline: Not Selected	IA-5(8)	IA-5(8)	IA-5(8)	IA-5(8)
IA-5(9)	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	NIST SP 800-53B R5 Baseline: Not Selected				
IA-5(10)	Authenticator Management | Dynamic Credential	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	NIST SP 800-53B R5 Baseline: Not Selected				
IA-5(11)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
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].	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	NIST SP 800-53B R5 Baseline: Not Selected				
IA-5(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	NIST SP 800-53B R5 Baseline: Not Selected				
IA-5(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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
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.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
IA-5(16)	Authenticator Management | In-person or Trusted External Party Authenticator	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	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
IA-5(17)	Authenticator Management | Presentation Attack Detection for Biometric	Employ presentation attack detection mechanisms for biometric-based authentication.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
IA-5(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	Functional	Equal	Password Managers	IAC-10.11	Mechanisms exist to protect and store passwords via a password manager tool.	10	NIST SP 800-53B R5 Baseline: Not Selected				
IA-6	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	NIST SP 800-53B R5 Baseline: Low	IA-6	IA-6	IA-6	
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.	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	NIST SP 800-53B R5 Baseline: Low	IA-7	IA-7	IA-7	IA-7
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.	Functional	Intersects With	Cryptographic Module Authentication	CRY-02	Automated mechanisms exist to enable systems to authenticate to a cryptographic module.	5	NIST SP 800-53B R5 Baseline: Low	IA-7	IA-7	IA-7	IA-7
IA-8	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	NIST SP 800-53B R5 Baseline: Low	IA-8	IA-8	IA-8	
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.	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	NIST SP 800-53B R5 Baseline: Low	IA-8(1)	IA-8(1)	IA-8(1)	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)	Low	Mod	High	Privacy
IA-8(2)	Identification and Authentication (non-organizational Users) | Acceptance of External	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	NIST SP 800-53B R5 Baseline: Low	IA-8(2)	IA-8(2)	IA-8(2)	
IA-8(3)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
IA-8(4)	Identification and Authentication (non-organizational Users) | Use of Defined	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	NIST SP 800-53B R5 Baseline: Low	IA-8(4)	IA-8(4)	IA-8(4)	
IA-8(5)	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	NIST SP 800-53B R5 Baseline: Not Selected				
IA-8(6)	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	NIST SP 800-53B R5 Baseline: Not Selected				
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.	Functional	Equal	Identification & Authentication for Third Party Systems & Services	IAC-05	Mechanisms exist to identify and authenticate third-party systems and services.	10	NIST SP 800-53B R5 Baseline: Not Selected				
IA-9(1)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
IA-9(2)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	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	Functional	Equal	Adaptive Identification & Authentication	IAC-13	Mechanisms exist to allow individuals to utilize alternative methods of authentication under specific circumstances or situations.	10	NIST SP 800-53B R5 Baseline: 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-	10	NIST SP 800-53B R5 Baseline: Low	IA-11	IA-11	IA-11	
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	NIST SP 800-53B R5 Baseline: Moderate		IA-12	IA-12	
IA-12(1)	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	NIST SP 800-53B R5 Baseline: Not Selected				
IA-12(2)	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	10	NIST SP 800-53B R5 Baseline: Moderate		IA-12(2)	IA-12(2)	
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].	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	NIST SP 800-53B R5 Baseline: Moderate		IA-12(3)	IA-12(3)	
IA-12(4)	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	NIST SP 800-53B R5 Baseline: High	IA-12(4)	IA-12(4)	IA-12(4)	IA-12(4)
IA-12(4)	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	NIST SP 800-53B R5 Baseline: High	IA-12(4)	IA-12(4)	IA-12(4)	IA-12(4)
IA-12(4)	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	NIST SP 800-53B R5 Baseline: High	IA-12(4)	IA-12(4)	IA-12(4)	IA-12(4)
IA-12(5)	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	10	NIST SP 800-53B R5 Baseline: Moderate		IA-12(5)	IA-12(5)	
IA-12(6)	Identity Proofing | Accept Externally-proofed Identities	Accept externally-proofed identities at [Assignment: organization-defined identity assurance level].	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
IA-13		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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
IA-13(1)		Cryptographic keys that protect access tokens are generated, managed, and protected from disclosure and misuse.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
IA-13(2)		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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
IA-13(3)		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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
IR-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] incident response policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 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:	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	NIST SP 800-53B R5 Baseline: Low	IR-1	IR-1	IR-1	IR-1
IR-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] incident response policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 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:	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 & data privacy-related incidents.	10	NIST SP 800-53B R5 Baseline: Low	IR-1	IR-1	IR-1	IR-1

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)	Low	Mod	High	Privacy
IR-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] incident response policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 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:	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	NIST SP 800-53B R5 Baseline: Low	IR-1	IR-1	IR-1	IR-1
IR-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] incident response policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 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:	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity & data privacy incidents to reduce the likelihood or impact of future incidents.	5	NIST SP 800-53B R5 Baseline: Low	IR-1	IR-1	IR-1	IR-1
IR-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] incident response policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 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:	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	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 continuing suitability, adequacy and effectiveness.	5	NIST SP 800-53B R5 Baseline: Low	IR-1	IR-1	IR-1	IR-1
IR-2	Incident Response Training	a. Provide incident response training to system users consistent with assigned roles and responsibilities:1. Within [Assignment: organization-defined time period] of assuming an incident response role or responsibility or acquiring system access;2. When required by system changes; 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	NIST SP 800-53B R5 Baseline: Low	IR-2	IR-2	IR-2	IR-2
IR-2(1)	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	10	NIST SP 800-53B R5 Baseline: High			IR-2(1)	
IR-2(2)	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	10	NIST SP 800-53B R5 Baseline: High			IR-2(2)	
IR-2(3)	Incident Response Training | Breach	Provide incident response training on how to identify and respond to a breach, including the organization's process for reporting a breach.	Functional	Intersects With	Incident Response Training	IRO-05	Mechanisms exist to train personnel in their incident response roles and responsibilities.	5	NIST SP 800-53B R5 Baseline: Not Selected				IR-2(3)
IR-3	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	NIST SP 800-53B R5 Baseline: Moderate		IR-3	IR-3	IR-3
IR-3(1)	Incident Response Testing | Automated Testing	Test the incident response capability using [Assignment: organization-defined automated mechanisms].	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
IR-3(2)	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	NIST SP 800-53B R5 Baseline: Moderate		IR-3(2)	IR-3(2)	
IR-3(3)	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	NIST SP 800-53B R5 Baseline: Not Selected				
IR-4	Incident Handling	a. Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery;b. Coordinate incident handling activities with contingency planning activities;c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly; 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	NIST SP 800-53B R5 Baseline: Low	IR-4	IR-4	IR-4	IR-4
IR-4(1)	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	NIST SP 800-53B R5 Baseline: Moderate		IR-4(1)	IR-4(1)	
IR-4(2)	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 information system components as part of the incident response capability.	10	NIST SP 800-53B R5 Baseline: Not Selected				
IR-4(3)	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 assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	5	NIST SP 800-53B R5 Baseline: Not Selected	IR-4(3)	IR-4(3)	IR-4(3)	IR-4(3)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)	Low	Mod	High	Privacy
IR-4(3)	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	NIST SP 800-53B R5 Baseline: Not Selected	IR-4(3)	IR-4(3)	IR-4(3)	IR-4(3)
IR-4(4)	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	NIST SP 800-53B R5 Baseline: High	IR-4(4)	IR-4(4)	IR-4(4)	IR-4(4)
IR-4(4)	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	5	NIST SP 800-53B R5 Baseline: High	IR-4(4)	IR-4(4)	IR-4(4)	IR-4(4)
IR-4(5)	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	Mechanisms exist to automatically implement pre-determined corrective actions in response to detected events that have security incident	5	NIST SP 800-53B R5 Baseline: Not Selected	IR-4(5)	IR-4(5)	IR-4(5)	IR-4(5)
IR-4(5)	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 System	IRO-02.6	Mechanisms exist to automatically disable systems, upon detection of a possible incident that meets organizational criteria, which allows for forensic analysis to be performed.	5	NIST SP 800-53B R5 Baseline: Not Selected	IR-4(5)	IR-4(5)	IR-4(5)	IR-4(5)
IR-4(6)	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	NIST SP 800-53B R5 Baseline: Not Selected				
IR-4(7)	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	NIST SP 800-53B R5 Baseline: Not Selected				
IR-4(8)	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	NIST SP 800-53B R5 Baseline: Not Selected				
IR-4(9)	Incident Handling | Dynamic Response Capability	Employ [Assignment: organization-defined dynamic response capabilities] to respond to incidents.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
IR-4(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	NIST SP 800-53B R5 Baseline: Not Selected	IR-4(10)	IR-4(10)	IR-4(10)	IR-4(10)
IR-4(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 & data privacy incident information to the provider of the product or service and other organizations involved in the supply chain for systems or system components related to the incident.	5	NIST SP 800-53B R5 Baseline: Not Selected	IR-4(10)	IR-4(10)	IR-4(10)	IR-4(10)
IR-4(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 & data privacy incident response operations.	10	NIST SP 800-53B R5 Baseline: High			IR-4(11)	
IR-4(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 & data privacy incidents to reduce the likelihood or impact of future incidents.	5	NIST SP 800-53B R5 Baseline: Not Selected	IR-4(12)	IR-4(12)	IR-4(12)	IR-4(12)
IR-4(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	NIST SP 800-53B R5 Baseline: Not Selected	IR-4(12)	IR-4(12)	IR-4(12)	IR-4(12)
IR-4(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	5	NIST SP 800-53B R5 Baseline: Not Selected	IR-4(13)	IR-4(13)	IR-4(13)	IR-4(13)
IR-4(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 detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	5	NIST SP 800-53B R5 Baseline: Not Selected	IR-4(13)	IR-4(13)	IR-4(13)	IR-4(13)
IR-4(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	NIST SP 800-53B R5 Baseline: Not Selected	IR-4(13)	IR-4(13)	IR-4(13)	IR-4(13)
IR-4(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	NIST SP 800-53B R5 Baseline: Not Selected				
IR-4(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	NIST SP 800-53B R5 Baseline: Not Selected				
IR-5	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 & data privacy incidents to internal stakeholders all the way through the resolution of the	10	NIST SP 800-53B R5 Baseline: Low	IR-5	IR-5	IR-5	IR-5
IR-5(1)	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 & data	10	NIST SP 800-53B R5 Baseline: High			IR-5(1)	
IR-6	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	5	NIST SP 800-53B R5 Baseline: Low	IR-6	IR-6	IR-6	IR-6
IR-6	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	Functional	Intersects With	Regulatory & Law Enforcement Contacts	IRO-14	Mechanisms exist to maintain incident response contacts with applicable regulatory and law enforcement agencies.	5	NIST SP 800-53B R5 Baseline: Low	IR-6	IR-6	IR-6	IR-6
IR-6	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	Functional	Intersects With	Contacts With Authorities	GOV-06	Mechanisms exist to identify and document appropriate contacts with relevant law enforcement and regulatory bodies.	5	NIST SP 800-53B R5 Baseline: Low	IR-6	IR-6	IR-6	IR-6
IR-6(1)	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 & data privacy	10	NIST SP 800-53B R5 Baseline: Moderate		IR-6(1)	IR-6(1)	
IR-6(2)	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 & data privacy incidents to reduce the likelihood or impact of future incidents.	5	NIST SP 800-53B R5 Baseline: Not Selected	IR-6(2)	IR-6(2)	IR-6(2)	IR-6(2)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)	Low	Mod	High	Privacy
IR-6(2)	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 & data privacy incidents to organization-defined personnel or roles.	5	NIST SP 800-53B R5 Baseline: Not Selected	IR-6(2)	IR-6(2)	IR-6(2)	IR-6(2)
IR-6(3)	Incident Reporting | Supply Chain Coordination	Provide incident information to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident.	Functional	Intersects With	Supply Chain Coordination	IRO-10.4	Mechanisms exist to provide cybersecurity & data privacy incident information to the provider of the product or service and other organizations involved in the supply chain for systems or system components related to the incident.	5	NIST SP 800-53B R5 Baseline: Moderate		IR-6(3)	IR-6(3)	
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.	Functional	Equal	Incident Reporting Assistance	IRO-11	Mechanisms exist to provide incident response advice and assistance to users of systems for the handling and reporting of actual and potential cybersecurity & data privacy	10	NIST SP 800-53B R5 Baseline: Low	IR-7	IR-7	IR-7	IR-7
IR-7(1)	Incident Response Assistance | Automation Support for Availability of Information and	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	NIST SP 800-53B R5 Baseline: Moderate		IR-7(1)	IR-7(1)	
IR-7(2)	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	NIST SP 800-53B R5 Baseline: Not Selected				
IR-8	Incident Response Plan	a. Develop an incident response plan that:1. Provides the organization with a roadmap for implementing its incident response capability;2. Describes the structure and organization of the incident response capability;3. Provides a high-level approach for how the incident response capability fits into the overall organization;4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;5. Defines reportable incidents;6. Provides metrics for measuring the incident response capability within the organization;7. Defines the resources and management support needed to effectively maintain and mature an incident response capability;8. Addresses the sharing of incident information;9. Is reviewed and approved by [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency]; 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	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	NIST SP 800-53B R5 Baseline: Low	IR-8	IR-8	IR-8	IR-8
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 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	NIST SP 800-53B R5 Baseline: Not Selected				IR-8(1)
IR-9	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	NIST SP 800-53B R5 Baseline: Not Selected	IR-9	IR-9	IR-9	IR-9
IR-9	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	NIST SP 800-53B R5 Baseline: Not Selected	IR-9	IR-9	IR-9	IR-9
IR-9(1)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
IR-9(2)	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	NIST SP 800-53B R5 Baseline: Not Selected				
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].	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 systems are undergoing corrective actions.	10	NIST SP 800-53B R5 Baseline: Not Selected				
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].	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	NIST SP 800-53B R5 Baseline: Not Selected				
IR-10	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
MA-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] maintenance policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 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	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	NIST SP 800-53B R5 Baseline: Low	MA-1	MA-1	MA-1	MA-1

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)	Low	Mod	High	Privacy
MA-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] maintenance policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 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	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	NIST SP 800-53B R5 Baseline: Low	MA-1	MA-1	MA-1	MA-1
MA-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] maintenance policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 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	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	NIST SP 800-53B R5 Baseline: Low	MA-1	MA-1	MA-1	MA-1
MA-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] maintenance policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 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	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	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 continuing suitability, adequacy and effectiveness.	5	NIST SP 800-53B R5 Baseline: Low	MA-1	MA-1	MA-1	MA-1
MA-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] maintenance policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 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	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	NIST SP 800-53B R5 Baseline: Low	MA-1	MA-1	MA-1	MA-1
MA-2	Controlled Maintenance	a. Schedule, document, and review records of maintenance, repair, and replacement on system components in accordance with manufacturer or vendor specifications and/or organizational requirements;b. Approve and monitor all maintenance activities, whether performed on site or remotely and whether the system or system components are serviced on site or removed to another location;c. Require that [Assignment: organization-defined personnel or roles] explicitly approve the removal of the system or system components from organizational facilities for off-site maintenance, repair, or replacement;d. Sanitize equipment to remove the following information from associated media prior to removal from organizational facilities for off-site maintenance, repair, or replacement: [Assignment: organization-defined information];e. Check all potentially impacted controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions; andf. Include the following information in organizational maintenance records:	Functional	Equal	Controlled Maintenance	MNT-02	Mechanisms exist to conduct controlled maintenance activities throughout the lifecycle of the system, application or service.	10	NIST SP 800-53B R5 Baseline: Low	MA-2	MA-2	MA-2	
MA-2(1)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
MA-2(2)	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	NIST SP 800-53B R5 Baseline: High			MA-2(2)	
MA-3	Maintenance Tools	a. Approve, control, and monitor the use of system maintenance tools; andb. Review previously approved system maintenance tools [Assignment: organization-defined	Functional	Intersects With	Maintenance Tools	MNT-04	Mechanisms exist to control and monitor the use of system maintenance tools.	5	NIST SP 800-53B R5 Baseline: Moderate		MA-3	MA-3	
MA-3(1)	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	10	NIST SP 800-53B R5 Baseline: Moderate		MA-3(1)	MA-3(1)	
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.	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	NIST SP 800-53B R5 Baseline: Moderate		MA-3(2)	MA-3(2)	
MA-3(3)	Maintenance Tools | Prevent Unauthorized Removal	Prevent the removal of maintenance equipment containing organizational information by:a. Verifying that there is no organizational information contained on the equipment;b. Sanitizing or destroying the equipment;c. Retaining the equipment within the facility; ord. Obtaining an exemption from [Assignment: organization-defined personnel or roles] explicitly authorizing removal of the equipment from the	Functional	Equal	Prevent Unauthorized Removal	MNT-04.3	Mechanisms exist to prevent or control the removal of equipment undergoing maintenance that containing organizational information.	10	NIST SP 800-53B R5 Baseline: Moderate		MA-3(3)	MA-3(3)	
MA-3(4)	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	NIST SP 800-53B R5 Baseline: Not Selected				
MA-3(5)	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	NIST SP 800-53B R5 Baseline: Not Selected				
MA-3(6)	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	NIST SP 800-53B R5 Baseline: 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 (optional)	Notes (optional)	Low	Mod	High	Privacy
MA-4	Nonlocal Maintenance	a. Approve and monitor nonlocal maintenance and diagnostic activities;b. Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system;c. Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions;d. Maintain records for nonlocal maintenance and diagnostic activities; ande. Terminate session and network connections when nonlocal	Functional	Intersects With	Remote Maintenance	MNT-05	Mechanisms exist to authorize, monitor and control remote, non-local maintenance and diagnostic activities.	5	NIST SP 800-53B R5 Baseline: Low	MA-4	MA-4	MA-4	MA-4
MA-4	Nonlocal Maintenance	a. Approve and monitor nonlocal maintenance and diagnostic activities;b. Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system;c. Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions;d. Maintain records for nonlocal maintenance and diagnostic activities; ande. Terminate session and network connections when nonlocal	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	NIST SP 800-53B R5 Baseline: Low	MA-4	MA-4	MA-4	MA-4
MA-4	Nonlocal Maintenance	a. Approve and monitor nonlocal maintenance and diagnostic activities;b. Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system;c. Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions;d. Maintain records for nonlocal maintenance and diagnostic activities; ande. Terminate session and network connections when nonlocal	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	NIST SP 800-53B R5 Baseline: Low	MA-4	MA-4	MA-4	MA-4
MA-4(1)	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	NIST SP 800-53B R5 Baseline: Not Selected				
MA-4(2)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
MA-4(3)	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 systems performing remote, non-local maintenance and / or diagnostic services implement a security capability comparable to the capability implemented on the system being serviced.	10	NIST SP 800-53B R5 Baseline: High			MA-4(3)	
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]; 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	NIST SP 800-53B R5 Baseline: Not Selected				
MA-4(5)	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	NIST SP 800-53B R5 Baseline: Not Selected				
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].	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	10	NIST SP 800-53B R5 Baseline: Not Selected				
MA-4(7)	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	NIST SP 800-53B R5 Baseline: Not Selected				
MA-5	Maintenance Personnel	a. Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel;b. Verify that non-escorted personnel performing maintenance on the system possess the required access authorizations; 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	Functional	Equal	Authorized Maintenance Personnel	MNT-06	Mechanisms exist to maintain a current list of authorized maintenance organizations or personnel.	10	NIST SP 800-53B R5 Baseline: Low	MA-5	MA-5	MA-5	
MA-5(1)	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	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	NIST SP 800-53B R5 Baseline: High			MA-5(1)	
MA-5(2)	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	5	NIST SP 800-53B R5 Baseline: Not Selected				
MA-5(3)	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	5	NIST SP 800-53B R5 Baseline: Not Selected				
MA-5(4)	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	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	NIST SP 800-53B R5 Baseline: Not Selected				
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.	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 IT systems have required access authorizations.	10	NIST SP 800-53B R5 Baseline: Not Selected				
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.	Functional	Equal	Timely Maintenance	MNT-03	Mechanisms exist to obtain maintenance support and/or spare parts for systems within a defined Recovery Time Objective (RTO).	10	NIST SP 800-53B R5 Baseline: Moderate		MA-6	MA-6	
MA-6(1)	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 systems, applications and services.	10	NIST SP 800-53B R5 Baseline: Not Selected				
MA-6(2)	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 systems, applications and services.	10	NIST SP 800-53B R5 Baseline: 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 (optional)	Notes (optional)	Low	Mod	High	Privacy
MA-6(3)	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	NIST SP 800-53B R5 Baseline: Not Selected				
MA-7	Field Maintenance	Restrict or prohibit field maintenance on [Assignment: organization-defined systems or system components] to [Assignment: organization-defined trusted maintenance	Functional	Equal	Field Maintenance	MNT-08	Mechanisms exist to securely conduct field maintenance on geographically deployed assets.	10	NIST SP 800-53B R5 Baseline: Not Selected				
MP-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] 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-	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	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 continuing suitability, adequacy and effectiveness.	5	NIST SP 800-53B R5 Baseline: Low	MP-1	MP-1	MP-1	MP-1
MP-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] 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-	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	NIST SP 800-53B R5 Baseline: Low	MP-1	MP-1	MP-1	MP-1
MP-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] 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-	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	NIST SP 800-53B R5 Baseline: Low	MP-1	MP-1	MP-1	MP-1
MP-2	Media Access	Restrict access to [Assignment: organization-defined types of digital and/or non-digital media] to [Assignment: organization-defined personnel or roles].	Functional	Intersects With	Media Access	DCH-03	Mechanisms exist to control and restrict access to digital and non-digital media to authorized	5	NIST SP 800-53B R5 Baseline: Low	MP-2	MP-2	MP-2	MP-2
MP-2	Media Access	Restrict access to [Assignment: organization-defined types of digital and/or non-digital media] to [Assignment: organization-defined personnel or roles].	Functional	Intersects With	Endpoint Security	END-01	Mechanisms exist to facilitate the implementation of endpoint security controls.	5	NIST SP 800-53B R5 Baseline: Low	MP-2	MP-2	MP-2	MP-2
MP-2(1)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
MP-2(2)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
MP-3	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	NIST SP 800-53B R5 Baseline: Moderate	MP-3	MP-3	MP-3	MP-3
MP-3	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	NIST SP 800-53B R5 Baseline: Moderate	MP-3	MP-3	MP-3	MP-3
MP-4	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,	10	NIST SP 800-53B R5 Baseline: Moderate		MP-4	MP-4	
MP-4(1)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
MP-4(2)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
MP-5	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	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	NIST SP 800-53B R5 Baseline: Moderate		MP-5	MP-5	
MP-5(1)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
MP-5(2)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
MP-5(3)	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	NIST SP 800-53B R5 Baseline: Not Selected				
MP-5(4)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
MP-6	Media Sanitization	a. Sanitize [Assignment: organization-defined system media] prior to disposal, release out of organizational control, or release for reuse using [Assignment: organization-defined sanitization techniques and procedures]; andb. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of	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	NIST SP 800-53B R5 Baseline: Low	MP-6	MP-6	MP-6	MP-6
MP-6	Media Sanitization	a. Sanitize [Assignment: organization-defined system media] prior to disposal, release out of organizational control, or release for reuse using [Assignment: organization-defined sanitization techniques and procedures]; andb. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of	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	5	NIST SP 800-53B R5 Baseline: Low	MP-6	MP-6	MP-6	MP-6

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)	Low	Mod	High	Privacy
MP-6	Media Sanitization	a. Sanitize [Assignment: organization-defined system media] prior to disposal, release out of organizational control, or release for reuse using [Assignment: organization-defined sanitization techniques and procedures]; andb. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of	Functional	Intersects With	Sanitization of Personal Data (PD)	DCH-09.3	Mechanisms exist to facilitate the sanitization of Personal Data (PD).	5	NIST SP 800-53B R5 Baseline: Low	MP-6	MP-6	MP-6	MP-6
MP-6(1)	Media Sanitization | Review, Approve, Track, Document, and	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	NIST SP 800-53B R5 Baseline: High			MP-6(1)	
MP-6(2)	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	NIST SP 800-53B R5 Baseline: High			MP-6(2)	
MP-6(3)	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	NIST SP 800-53B R5 Baseline: High	MP-6(3)	MP-6(3)	MP-6(3)	MP-6(3)
MP-6(3)	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	5	NIST SP 800-53B R5 Baseline: High	MP-6(3)	MP-6(3)	MP-6(3)	MP-6(3)
MP-6(3)	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	NIST SP 800-53B R5 Baseline: High	MP-6(3)	MP-6(3)	MP-6(3)	MP-6(3)
MP-6(4)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
MP-6(5)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
MP-6(6)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
MP-6(7)	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 /	10	NIST SP 800-53B R5 Baseline: Not Selected				
MP-6(8)	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	NIST SP 800-53B R5 Baseline: Not Selected				
MP-7	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	NIST SP 800-53B R5 Baseline: Low	MP-7	MP-7	MP-7	MP-7
MP-7	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	NIST SP 800-53B R5 Baseline: Low	MP-7	MP-7	MP-7	MP-7
MP-7	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 information systems when such devices have no identifiable owner.	5	NIST SP 800-53B R5 Baseline: Low	MP-7	MP-7	MP-7	MP-7
MP-7(1)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
MP-7(2)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
MP-8	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 systems, applications and services, commensurate with the security category and/or classification level of the information.	5	NIST SP 800-53B R5 Baseline: Not Selected				
MP-8(1)	Media Downgrading | Documentation of Process	Document system media downgrading actions.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
MP-8(2)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
MP-8(3)	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 systems, applications and services, commensurate with the security category and/or classification level of the information.	5	NIST SP 800-53B R5 Baseline: Not Selected				
MP-8(4)	Media Downgrading | Classified Information	Downgrade system media containing classified information prior to release to individuals without required access	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
PE-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] physical and environmental protection policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 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	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	NIST SP 800-53B R5 Baseline: Low	PE-1	PE-1	PE-1	PE-1
PE-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] physical and environmental protection policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 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	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	NIST SP 800-53B R5 Baseline: Low	PE-1	PE-1	PE-1	PE-1

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)	Low	Mod	High	Privacy
PE-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] physical and environmental protection policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 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	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	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 continuing suitability, adequacy and effectiveness.	5	NIST SP 800-53B R5 Baseline: Low	PE-1	PE-1	PE-1	PE-1
PE-2	Physical Access Authorizations	a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides;b. Issue authorization credentials for facility access;c. Review the access list detailing authorized facility access by individuals [Assignment: organization-defined frequency]; andd. Remove individuals from the facility access list when access is no	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	10	NIST SP 800-53B R5 Baseline: Low	PE-2	PE-2	PE-2	
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.	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	NIST SP 800-53B R5 Baseline: Not Selected				
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].	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	NIST SP 800-53B R5 Baseline: Not Selected				
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 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	NIST SP 800-53B R5 Baseline: Not Selected				
PE-3	Physical Access Control	a. Enforce physical access authorizations at [Assignment: organization-defined entry and exit points to the facility where the system resides] by:1. Verifying individual access authorizations before granting access to the facility; 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	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	NIST SP 800-53B R5 Baseline: Low	PE-3	PE-3	PE-3	
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].	Functional	Equal	Access To Information Systems	PES-03.4	Physical access control mechanisms exist to enforce physical access to critical information systems or sensitive/regulated data, in addition to the physical access controls for the facility.	10	NIST SP 800-53B R5 Baseline: High			PE-3(1)	
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.	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	5	NIST SP 800-53B R5 Baseline: Not Selected				
PE-3(3)	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	5	NIST SP 800-53B R5 Baseline: Not Selected				
PE-3(4)	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	NIST SP 800-53B R5 Baseline: Not Selected				
PE-3(5)	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	NIST SP 800-53B R5 Baseline: Not Selected				
PE-3(6)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
PE-3(7)	Physical Access Control | Physical Barriers	Limit access using physical barriers.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
PE-3(8)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
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].	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,	10	NIST SP 800-53B R5 Baseline: Moderate		PE-4	PE-4	
PE-5	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	NIST SP 800-53B R5 Baseline: Moderate		PE-5	PE-5	
PE-5(1)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
PE-5(2)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
PE-5(3)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
PE-6	Monitoring Physical Access	a. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents;b. Review physical access logs [Assignment: organization-defined frequency] and upon occurrence of [Assignment: organization-defined events or potential indications of events]; 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	NIST SP 800-53B R5 Baseline: Low	PE-6	PE-6	PE-6	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)	Low	Mod	High	Privacy
PE-6(1)	Monitoring Physical Access | Intrusion Alarms and Surveillance	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	NIST SP 800-53B R5 Baseline: Moderate		PE-6(1)	PE-6(1)	
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].	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
PE-6(3)	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	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
PE-6(4)	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 Information Systems	PES-05.2	Facility security mechanisms exist to monitor physical access to critical information systems or sensitive/regulated data, in addition to the physical access monitoring of the facility.	10	NIST SP 800-53B R5 Baseline: High			PE-6(4)	
PE-7	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
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]; andc. Report anomalies in visitor access records to [Assignment: organization-defined	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	NIST SP 800-53B R5 Baseline: Low	PE-8	PE-8	PE-8	
PE-8(1)	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	NIST SP 800-53B R5 Baseline: High			PE-8(1)	
PE-8(2)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
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].	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	NIST SP 800-53B R5 Baseline: Not Selected				PE-8(3)
PE-9	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	NIST SP 800-53B R5 Baseline: Moderate		PE-9	PE-9	
PE-9(1)	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	10	NIST SP 800-53B R5 Baseline: Not Selected				
PE-9(2)	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	NIST SP 800-53B R5 Baseline: 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	10	NIST SP 800-53B R5 Baseline: Moderate		PE-10	PE-10	
PE-10(1)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	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	NIST SP 800-53B R5 Baseline: Moderate		PE-11	PE-11	
PE-11(1)	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	NIST SP 800-53B R5 Baseline: High			PE-11(1)	
PE-11(2)	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	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	NIST SP 800-53B R5 Baseline: 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	10	NIST SP 800-53B R5 Baseline: Low	PE-12	PE-12	PE-12	
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.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: 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	NIST SP 800-53B R5 Baseline: Low	PE-13	PE-13	PE-13	
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.	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	10	NIST SP 800-53B R5 Baseline: Moderate		PE-13(1)	PE-13(1)	
PE-13(2)	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	Functional	Intersects With	Automatic Fire Suppression	PES-08.3	Facility security mechanisms exist to employ an automatic fire suppression capability for critical information systems when the facility is not staffed on a continuous basis.	5	NIST SP 800-53B R5 Baseline: High	PE-13(2)	PE-13(2)	PE-13(2)	PE-13(2)
PE-13(2)	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	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	5	NIST SP 800-53B R5 Baseline: High	PE-13(2)	PE-13(2)	PE-13(2)	PE-13(2)
PE-13(3)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
PE-13(4)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: 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	NIST SP 800-53B R5 Baseline: Low	PE-14	PE-14	PE-14	
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].	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
PE-14(2)	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	NIST SP 800-53B R5 Baseline: 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 (optional)	Notes (optional)	Low	Mod	High	Privacy
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	NIST SP 800-53B R5 Baseline: Low	PE-15	PE-15	PE-15	
PE-15(1)	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 information systems and alert facility maintenance and IT personnel.	10	NIST SP 800-53B R5 Baseline: High			PE-15(1)	
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	NIST SP 800-53B R5 Baseline: Low	PE-16	PE-16	PE-16	
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	NIST SP 800-53B R5 Baseline: Moderate		PE-17	PE-17	
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	5	NIST SP 800-53B R5 Baseline: High			PE-18	
PE-18(1)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
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	NIST SP 800-53B R5 Baseline: Not Selected				
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 the information.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: 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	10	NIST SP 800-53B R5 Baseline: 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	NIST SP 800-53B R5 Baseline: 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 cybersecurity & data privacy control applicability by identifying, assigning and documenting the appropriate asset scope categorization for all systems, applications, services and personnel (internal and third-parties).	5	NIST SP 800-53B R5 Baseline: Not Selected	PE-22	PE-22	PE-22	PE-22
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	5	NIST SP 800-53B R5 Baseline: Not Selected	PE-22	PE-22	PE-22	PE-22
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	NIST SP 800-53B R5 Baseline: Not Selected	PE-23	PE-23	PE-23	PE-23
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	NIST SP 800-53B R5 Baseline: Not Selected	PE-23	PE-23	PE-23	PE-23
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	5	NIST SP 800-53B R5 Baseline: Not Selected	PE-23	PE-23	PE-23	PE-23
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	NIST SP 800-53B R5 Baseline: Not Selected	PE-23	PE-23	PE-23	PE-23
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	5	NIST SP 800-53B R5 Baseline: Not Selected	PE-23	PE-23	PE-23	PE-23
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	NIST SP 800-53B R5 Baseline: Not Selected	PE-23	PE-23	PE-23	PE-23
PL-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] planning policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 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:	Functional	Subset Of	Cybersecurity & Data Privacy Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of cybersecurity & data privacy-related resource planning controls that define a viable plan for achieving cybersecurity & data privacy objectives.	10	NIST SP 800-53B R5 Baseline: Low	PL-1	PL-1	PL-1	PL-1
PL-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] planning policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 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:	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	NIST SP 800-53B R5 Baseline: Low	PL-1	PL-1	PL-1	PL-1

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)	Low	Mod	High	Privacy
PL-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] planning policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 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:	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	NIST SP 800-53B R5 Baseline: Low	PL-1	PL-1	PL-1	PL-1
PL-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] planning policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 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:	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	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 continuing suitability, adequacy and effectiveness.	5	NIST SP 800-53B R5 Baseline: Low	PL-1	PL-1	PL-1	PL-1
PL-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] planning policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 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:	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	NIST SP 800-53B R5 Baseline: Low	PL-1	PL-1	PL-1	PL-1
PL-2	System Security and Privacy Plans	a. Develop security and privacy plans for the system that:1. Are consistent with the organization's enterprise architecture;2. Explicitly define the constituent system components;3. Describe the operational context of the system in terms of mission and business processes;4. Identify the individuals that fulfill system roles and responsibilities;5. Identify the information types processed, stored, and transmitted by the system;6. Provide the security categorization of the system, including supporting rationale;7. Describe any specific threats to the system that are of concern to the organization;8. Provide the results of a privacy risk assessment for systems processing personally identifiable information;9. Describe the operational environment for the system and any dependencies on or connections to other systems or system components;10. Provide an overview of the security and privacy requirements for the system;11. Identify any relevant control baselines or overlays, if applicable;12. Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions;13. Include risk determinations for security and privacy architecture and design decisions;14. Include security- and privacy-related activities affecting the system that require planning and coordination with [Assignment: organization-defined individuals or groups]; 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	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	NIST SP 800-53B R5 Baseline: Low	PL-2	PL-2	PL-2	PL-2
PL-2	System Security and Privacy Plans	a. Develop security and privacy plans for the system that:1. Are consistent with the organization's enterprise architecture;2. Explicitly define the constituent system components;3. Describe the operational context of the system in terms of mission and business processes;4. Identify the individuals that fulfill system roles and responsibilities;5. Identify the information types processed, stored, and transmitted by the system;6. Provide the security categorization of the system, including supporting rationale;7. Describe any specific threats to the system that are of concern to the organization;8. Provide the results of a privacy risk assessment for systems processing personally identifiable information;9. Describe the operational environment for the system and any dependencies on or connections to other systems or system components;10. Provide an overview of the security and privacy requirements for the system;11. Identify any relevant control baselines or overlays, if applicable;12. Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions;13. Include risk determinations for security and privacy architecture and design decisions;14. Include security- and privacy-related activities affecting the system that require planning and coordination with [Assignment: organization-defined individuals or groups]; 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	Functional	Intersects With	System Security & Privacy Plan (SSPP)	IAO-03	Mechanisms exist to generate System Security & Privacy Plans (SSPPs), or similar document repositories, to identify and maintain key architectural information on each critical system, application or service, as well as influence inputs, entities, systems, applications and processes, providing a historical record of the data and its origins.	5	NIST SP 800-53B R5 Baseline: Low	PL-2	PL-2	PL-2	PL-2

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)	Low	Mod	High	Privacy
PL-2	System Security and Privacy Plans	a. Develop security and privacy plans for the system that:1. Are consistent with the organization's enterprise architecture;2. Explicitly define the constituent system components;3. Describe the operational context of the system in terms of mission and business processes;4. Identify the individuals that fulfill system roles and responsibilities;5. Identify the information types processed, stored, and transmitted by the system;6. Provide the security categorization of the system, including supporting rationale;7. Describe any specific threats to the system that are of concern to the organization;8. Provide the results of a privacy risk assessment for systems processing personally identifiable information;9. Describe the operational environment for the system and any dependencies on or connections to other systems or system components;10. Provide an overview of the security and privacy requirements for the system;11. Identify any relevant control baselines or overlays, if applicable;12. Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions;13. Include risk determinations for security and privacy architecture and design decisions;14. Include security- and privacy-related activities affecting the system that require planning and coordination with [Assignment: organization-defined individuals or groups]; 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	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	NIST SP 800-53B R5 Baseline: Low	PL-2	PL-2	PL-2	PL-2
PL-2(1)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
PL-2(2)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
PL-2(3)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
PL-3	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
PL-4	Rules of Behavior	a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy;b. Receive a documented acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system;c. Review and update the rules of behavior [Assignment: organization-defined frequency]; 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	Functional	Intersects With	Terms of Employment	HRS-05	Mechanisms exist to require all employees and contractors to apply cybersecurity & data privacy principles in their daily work.	5	NIST SP 800-53B R5 Baseline: Low	PL-4	PL-4	PL-4	PL-4
PL-4	Rules of Behavior	a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy;b. Receive a documented acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system;c. Review and update the rules of behavior [Assignment: organization-defined frequency]; 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	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	NIST SP 800-53B R5 Baseline: Low	PL-4	PL-4	PL-4	PL-4
PL-4	Rules of Behavior	a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy;b. Receive a documented acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system;c. Review and update the rules of behavior [Assignment: organization-defined frequency]; 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	Functional	Intersects With	Use of Communications Technology	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for communications technologies based on the potential to cause damage to systems, if used maliciously.	5	NIST SP 800-53B R5 Baseline: Low	PL-4	PL-4	PL-4	PL-4
PL-4(1)	Rules of Behavior | Social Media and External Site/application Usage Restrictions	Include in the rules of behavior, restrictions on:a. Use of social media, social networking sites, and external sites/applications;b. Posting organizational information on public websites; andc. Use of organization-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external	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	NIST SP 800-53B R5 Baseline: Low	PL-4(1)	PL-4(1)	PL-4(1)	PL-4(1)
PL-5	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
PL-6	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
PL-7	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	10	NIST SP 800-53B R5 Baseline: Not Selected				
PL-8	Security and Privacy Architectures	a. Develop security and privacy architectures for the system that:1. Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information;2. Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals;3. Describe how the architectures are integrated into and support the enterprise architecture; 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	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 cybersecurity & data privacy principles that addresses risk to organizational operations, assets, individuals, other organizations.	5	NIST SP 800-53B R5 Baseline: Moderate		PL-8	PL-8	PL-8
PL-8(1)	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	NIST SP 800-53B R5 Baseline: Not Selected				
PL-8(2)	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 cybersecurity & data privacy technologies from different suppliers to minimize supply chain risk.	5	NIST SP 800-53B R5 Baseline: Not Selected				
PL-9	Central Management	Centrally manage [Assignment: organization-defined controls and related processes].	Functional	Intersects With	Centralized Management of Cybersecurity & Data Privacy Controls	SEA-01.1	Mechanisms exist to centrally-manage the organization-wide management and implementation of cybersecurity & data privacy controls	5	NIST SP 800-53B R5 Baseline: Not Selected	PL-9	PL-9	PL-9	PL-9
PL-9	Central Management	Centrally manage [Assignment: organization-defined controls and related processes].	Functional	Intersects With	Centralized Management of Flaw Remediation	VPM-05.1	Mechanisms exist to centrally-manage the flaw remediation process.	5	NIST SP 800-53B R5 Baseline: Not Selected	PL-9	PL-9	PL-9	PL-9

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)	Low	Mod	High	Privacy
PL-9	Central Management	Centrally manage [Assignment: organization-defined controls and related processes].	Functional	Intersects With	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 & data protection program.	5	NIST SP 800-53B R5 Baseline: Not Selected	PL-9	PL-9	PL-9	PL-9
PL-9	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	NIST SP 800-53B R5 Baseline: Not Selected	PL-9	PL-9	PL-9	PL-9
PL-9	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	NIST SP 800-53B R5 Baseline: Not Selected	PL-9	PL-9	PL-9	PL-9
PL-9	Central Management	Centrally manage [Assignment: organization-defined controls and related processes].	Functional	Intersects With	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 information system	5	NIST SP 800-53B R5 Baseline: Not Selected	PL-9	PL-9	PL-9	PL-9
PL-10	Baseline Selection	Select a control baseline for the system.	Functional	Equal	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	10	NIST SP 800-53B R5 Baseline: Low	PL-10	PL-10	PL-10	
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	10	NIST SP 800-53B R5 Baseline: Low	PL-11	PL-11	PL-11	
PM-1	Information Security Program Plan	a. Develop and disseminate an organization-wide information security program plan that:1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance;3. Reflects the coordination among organizational entities responsible for information security; 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	Functional	Subset Of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	NIST SP 800-53B R5 Baseline: Not Associated	PM-1	PM-1	PM-1	PM-1
PM-1	Information Security Program Plan	a. Develop and disseminate an organization-wide information security program plan that:1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance;3. Reflects the coordination among organizational entities responsible for information security; 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	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	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 continuing suitability, adequacy and effectiveness.	5	NIST SP 800-53B R5 Baseline: Not Associated	PM-1	PM-1	PM-1	PM-1
PM-1	Information Security Program Plan	a. Develop and disseminate an organization-wide information security program plan that:1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance;3. Reflects the coordination among organizational entities responsible for information security; 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	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	NIST SP 800-53B R5 Baseline: Not Associated	PM-1	PM-1	PM-1	PM-1
PM-2	Information Security Program Leadership Role	Appoint a senior agency information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.	Functional	Intersects With	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 & data protection program.	5	NIST SP 800-53B R5 Baseline: Not Associated				
PM-3	Information Security and Privacy Resources	a. Include the resources needed to implement the information security and privacy programs in capital planning and investment requests and document all exceptions to this requirement;b. Prepare documentation required for addressing information security and privacy programs in capital planning and investment requests in accordance with applicable laws, executive orders, directives, policies, regulations, standards; andc. Make available for expenditure, the planned information security and privacy resources.	Functional	Equal	Cybersecurity & Data Privacy Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the cybersecurity & data privacy programs and document all exceptions to this requirement.	10	NIST SP 800-53B R5 Baseline: Not Associated				PM-3
PM-4	Plan of Action and Milestones Process	a. Implement a process to ensure that plans of action and milestones for the information security, privacy, and supply chain risk management programs and associated organizational systems:1. Are developed and maintained;2. Document the remedial information security, privacy, and supply chain risk management actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; 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	NIST SP 800-53B R5 Baseline: Not Associated	PM-4	PM-4	PM-4	PM-4

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)	Low	Mod	High	Privacy
PM-4	Plan of Action and Milestones Process	a. Implement a process to ensure that plans of action and milestones for the information security, privacy, and supply chain risk management programs and associated organizational systems:1. Are developed and maintained;2. Document the remedial information security, privacy, and supply chain risk management actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; 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	Plan of Action & Milestones (POA&M)	IAO-05	Mechanisms exist to generate a Plan of Action and Milestones (POA&M), or similar risk register, 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.	5	NIST SP 800-53B R5 Baseline: Not Associated	PM-4	PM-4	PM-4	PM-4
PM-5	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	NIST SP 800-53B R5 Baseline: Not Associated	PM-5	PM-5	PM-5	PM-5
PM-5	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 that: (1) Accurately reflects the current systems, applications and services 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	5	NIST SP 800-53B R5 Baseline: Not Associated	PM-5	PM-5	PM-5	PM-5
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 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 systems, applications and services that collect, receive, process, store, transmit, update and/or share Personal Data (PD).	5	NIST SP 800-53B R5 Baseline: Not Associated	PM-5(1)	PM-5(1)	PM-5(1)	PM-5(1)
PM-5(1)	System Inventory | 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	NIST SP 800-53B R5 Baseline: Not Associated	PM-5(1)	PM-5(1)	PM-5(1)	PM-5(1)
PM-6	Measures of Performance	Develop, monitor, and report on the results of information security and privacy measures of performance.	Functional	Intersects With	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 & data protection program.	5	NIST SP 800-53B R5 Baseline: Not Associated	PM-6	PM-6	PM-6	PM-6
PM-6	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 cybersecurity & data privacy program measures of performance.	5	NIST SP 800-53B R5 Baseline: Not Associated	PM-6	PM-6	PM-6	PM-6
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.	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 cybersecurity & data privacy principles that addresses risk to organizational operations, assets,	5	NIST SP 800-53B R5 Baseline: Not Associated				PM-7
PM-7(1)	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	NIST SP 800-53B R5 Baseline: Not Associated				
PM-8	Critical Infrastructure Plan	Address information security and privacy issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	5	NIST SP 800-53B R5 Baseline: Not Associated	PM-8	PM-8	PM-8	PM-8
PM-8	Critical Infrastructure Plan	Address information security and privacy issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.	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	NIST SP 800-53B R5 Baseline: Not Associated	PM-8	PM-8	PM-8	PM-8
PM-9	Risk Management Strategy	a. Develops a comprehensive strategy to manage:1. Security risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of organizational systems; 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	Functional	Equal	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	NIST SP 800-53B R5 Baseline: Not Associated				PM-9
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	Functional	Equal	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of cybersecurity & data privacy assessment and authorization controls.	10	NIST SP 800-53B R5 Baseline: Not Associated				PM-10
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 cybersecurity & data privacy 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	NIST SP 800-53B R5 Baseline: Not Associated				PM-11
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	NIST SP 800-53B R5 Baseline: 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	NIST SP 800-53B R5 Baseline: Not Associated	PM-13	PM-13	PM-13	PM-13
PM-13	Security and Privacy Workforce	Establish a security and privacy workforce development and improvement program.	Functional	Intersects With	Cybersecurity & Data Privacy-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness	5	NIST SP 800-53B R5 Baseline: Not Associated	PM-13	PM-13	PM-13	PM-13
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	Testing, Training & Monitoring	PRI-08	Mechanisms exist to conduct cybersecurity & data privacy testing, training and monitoring activities	5	NIST SP 800-53B R5 Baseline: Not Associated	PM-14	PM-14	PM-14	PM-14

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)	Low	Mod	High	Privacy
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	Cybersecurity & Data Protection Controls Oversight	CPL-02	Mechanisms exist to provide a cybersecurity & data protection controls oversight function that reports to the organization's executive leadership.	5	NIST SP 800-53B R5 Baseline: Not Associated	PM-14	PM-14	PM-14	PM-14
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 Feeds 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	5	NIST SP 800-53B R5 Baseline: Not Associated	PM-15	PM-15	PM-15	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; 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 cybersecurity & data privacy communities to: (1) Facilitate ongoing cybersecurity & data privacy education and training for organizational personnel; (2) Maintain currency with recommended cybersecurity & data privacy practices, techniques and technologies; and (3) Share current cybersecurity and/or data privacy-related information including threats, vulnerabilities and incidents.	5	NIST SP 800-53B R5 Baseline: Not Associated	PM-15	PM-15	PM-15	PM-15
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 Feeds 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	5	NIST SP 800-53B R5 Baseline: Not Associated				
PM-16(1)	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 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	5	NIST SP 800-53B R5 Baseline: 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 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 systems, are implemented in accordance with applicable statutory, regulatory and contractual	10	NIST SP 800-53B R5 Baseline: Not Associated				PM-17
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	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	NIST SP 800-53B R5 Baseline: Not Associated				PM-18
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	NIST SP 800-53B R5 Baseline: Not Associated				PM-19
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	10	NIST SP 800-53B R5 Baseline: Not Associated				PM-20

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)	Low	Mod	High	Privacy
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; 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 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 (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	NIST SP 800-53B R5 Baseline: Not Associated				PM-20(1)
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	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	NIST SP 800-53B R5 Baseline: Not Associated				PM-21
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	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	NIST SP 800-53B R5 Baseline: Not Associated	PM-22	PM-22	PM-22	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 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	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	NIST SP 800-53B R5 Baseline: Not Associated	PM-22	PM-22	PM-22	PM-22
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	5	NIST SP 800-53B R5 Baseline: Not Associated	PM-23	PM-23	PM-23	PM-23
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	NIST SP 800-53B R5 Baseline: Not Associated	PM-23	PM-23	PM-23	PM-23
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	5	NIST SP 800-53B R5 Baseline: Not Associated	PM-23	PM-23	PM-23	PM-23
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	5	NIST SP 800-53B R5 Baseline: Not Associated	PM-24	PM-24	PM-24	PM-24
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	5	NIST SP 800-53B R5 Baseline: Not Associated	PM-24	PM-24	PM-24	PM-24
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	NIST SP 800-53B R5 Baseline: Not Associated	PM-24	PM-24	PM-24	PM-24
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 (2) Remediating identified inaccuracies, as necessary.	5	NIST SP 800-53B R5 Baseline: Not Associated	PM-24	PM-24	PM-24	PM-24
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	NIST SP 800-53B R5 Baseline: Not Associated	PM-24	PM-24	PM-24	PM-24
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, based on updated data subject	5	NIST SP 800-53B R5 Baseline: Not Associated	PM-24	PM-24	PM-24	PM-24
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, updating and/or sharing 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 (3) What is consistent with applicable laws, regulations and contractual obligations.	5	NIST SP 800-53B R5 Baseline: Not Associated	PM-25	PM-25	PM-25	PM-25

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)	Low	Mod	High	Privacy
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	NIST SP 800-53B R5 Baseline: Not Associated	PM-25	PM-25	PM-25	PM-25
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	NIST SP 800-53B R5 Baseline: Not Associated	PM-25	PM-25	PM-25	PM-25
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	5	NIST SP 800-53B R5 Baseline: Not Associated	PM-25	PM-25	PM-25	PM-25
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	NIST SP 800-53B R5 Baseline: Not Associated	PM-25	PM-25	PM-25	PM-25
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	Functional	Intersects With	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to complaints, concerns or questions from authenticated data subjects about how the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes of their Personal Data (PD).	5	NIST SP 800-53B R5 Baseline: Not Associated	PM-26	PM-26	PM-26	PM-26
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	Functional	Intersects With	Appeal Adverse Decision	PRI-06.3	Mechanisms exist to maintain a process for data subjects to appeal an adverse decision.	5	NIST SP 800-53B R5 Baseline: Not Associated	PM-26	PM-26	PM-26	PM-26
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 cover collecting, receiving, processing, storing, transmitting, updating, sharing and disposal actions with sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual requirements.	10	NIST SP 800-53B R5 Baseline: Not Associated				PM-27
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	NIST SP 800-53B R5 Baseline: Not Associated				PM-28
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 systems, system components and services, including documenting selected mitigating actions and monitoring performance against	5	NIST SP 800-53B R5 Baseline: Not Associated	PM-29	PM-29	PM-29	PM-29
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 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 & data protection program.	5	NIST SP 800-53B R5 Baseline: Not Associated	PM-29	PM-29	PM-29	PM-29
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	Functional	Intersects With	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	5	NIST SP 800-53B R5 Baseline: Not Associated	PM-29	PM-29	PM-29	PM-29
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 systems, system components and services, including documenting selected mitigating actions and monitoring performance against	10	NIST SP 800-53B R5 Baseline: Not Associated				
PM-30(1)	Supply Chain Risk Management Strategy | Suppliers of Critical or Mission-essential	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	NIST SP 800-53B R5 Baseline: Not Associated	PM-30(1)	PM-30(1)	PM-30(1)	PM-30(1)
PM-30(1)	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	TDA-06.1	Mechanisms exist to require the developer of the system, system component or service to perform a criticality analysis at organization-defined decision points in the Secure Development Life Cycle (SDLC).	5	NIST SP 800-53B R5 Baseline: Not Associated	PM-30(1)	PM-30(1)	PM-30(1)	PM-30(1)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)	Low	Mod	High	Privacy
PM-30(1)	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 systems, components and services using a supply chain risk assessment process relative to their importance in supporting the delivery of high-	5	NIST SP 800-53B R5 Baseline: Not Associated	PM-30(1)	PM-30(1)	PM-30(1)	PM-30(1)
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	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	NIST SP 800-53B R5 Baseline: Not Associated				PM-31
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 services or functions to ensure those resources are being used consistent with their intended purpose.	10	NIST SP 800-53B R5 Baseline: Not Associated				
PS-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] personnel security policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 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:	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	NIST SP 800-53B R5 Baseline: Low	PS-1	PS-1	PS-1	PS-1
PS-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] personnel security policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 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:	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	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 continuing suitability, adequacy and effectiveness.	5	NIST SP 800-53B R5 Baseline: Low	PS-1	PS-1	PS-1	PS-1
PS-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] personnel security policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 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:	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	NIST SP 800-53B R5 Baseline: Low	PS-1	PS-1	PS-1	PS-1
PS-2	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	NIST SP 800-53B R5 Baseline: Low	PS-2	PS-2	PS-2	PS-2
PS-2	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	NIST SP 800-53B R5 Baseline: Low	PS-2	PS-2	PS-2	PS-2
PS-3	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	Functional	Equal	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	10	NIST SP 800-53B R5 Baseline: Low	PS-3	PS-3	PS-3	
PS-3(1)	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	NIST SP 800-53B R5 Baseline: Not Selected				
PS-3(2)	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	NIST SP 800-53B R5 Baseline: Not Selected				
PS-3(3)	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	NIST SP 800-53B R5 Baseline: Not Selected				
PS-3(4)	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	10	NIST SP 800-53B R5 Baseline: 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 (optional)	Notes (optional)	Low	Mod	High	Privacy
PS-4	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	NIST SP 800-53B R5 Baseline: Low	PS-4	PS-4	PS-4	
PS-4(1)	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	HRS-09.3	Mechanisms exist to govern former employee behavior by notifying terminated individuals of applicable, legally binding post-employment requirements for the protection of organizational information.	10	NIST SP 800-53B R5 Baseline: Not Selected				
PS-4(2)	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	Automated mechanisms exist to notify Identity and Access Management (IAM) personnel or roles upon termination of an individual	10	NIST SP 800-53B R5 Baseline: High			PS-4(2)	
PS-5	Personnel Transfer	a. Review and confirm ongoing operational need for current logical and physical access authorizations to systems and facilities when individuals are reassigned or transferred to other positions within the organization;b. Initiate [Assignment: organization-defined transfer or reassignment actions] within [Assignment: organization-defined time period following the formal transfer action];c. Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; 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 systems and facilities upon personnel reassignment or transfer, in a timely manner.	10	NIST SP 800-53B R5 Baseline: Low	PS-5	PS-5	PS-5	
PS-6	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	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	NIST SP 800-53B R5 Baseline: Low	PS-6	PS-6	PS-6	PS-6
PS-6	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	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	NIST SP 800-53B R5 Baseline: Low	PS-6	PS-6	PS-6	PS-6
PS-6(1)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
PS-6(2)	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	NIST SP 800-53B R5 Baseline: Not Selected	PS-6(2)	PS-6(2)	PS-6(2)	PS-6(2)
PS-6(2)	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	NIST SP 800-53B R5 Baseline: Not Selected	PS-6(2)	PS-6(2)	PS-6(2)	PS-6(2)
PS-6(3)	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 Obligations	HRS-06.2	Mechanisms exist to notify terminated individuals of applicable, legally-binding post-employment requirements for the protection of sensitive organizational information.	10	NIST SP 800-53B R5 Baseline: Not Selected				
PS-7	External Personnel Security	a. Establish personnel security requirements, including security roles and responsibilities for external providers;b. Require external providers to comply with personnel security policies and procedures established by the organization;c. Document personnel security requirements;d. Require external providers to notify [Assignment: organization-defined personnel or roles] of any personnel transfers or terminations of external personnel who possess organizational credentials and/or badges, or who have system privileges within [Assignment: organization-defined time period]; ande. Monitor provider compliance with personnel security requirements.	Functional	Equal	Third-Party Personnel Security	HRS-10	Mechanisms exist to govern third-party personnel by reviewing and monitoring third-party cybersecurity & data privacy roles and responsibilities.	10	NIST SP 800-53B R5 Baseline: Low	PS-7	PS-7	PS-7	
PS-8	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	NIST SP 800-53B R5 Baseline: Low	PS-8	PS-8	PS-8	
PS-9	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	NIST SP 800-53B R5 Baseline: Low	PS-9	PS-9	PS-9	
PT-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] 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	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	NIST SP 800-53B R5 Baseline: Not Selected	PT-1	PT-1	PT-1	PT-1

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)	Low	Mod	High	Privacy
PT-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] 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	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	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 continuing suitability, adequacy and effectiveness.	5	NIST SP 800-53B R5 Baseline: Not Selected	PT-1	PT-1	PT-1	PT-1
PT-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] 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	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	NIST SP 800-53B R5 Baseline: Not Selected	PT-1	PT-1	PT-1	PT-1
PT-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] 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	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity & data privacy practices in the specification, design, development, implementation and modification of systems and services.	10	NIST SP 800-53B R5 Baseline: Not Selected	PT-1	PT-1	PT-1	PT-1
PT-2	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, update and/or share Personal Data (PD), either generally or in support of a specific business process.	5	NIST SP 800-53B R5 Baseline: Not Selected	PT-2	PT-2	PT-2	PT-2
PT-2	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	5	NIST SP 800-53B R5 Baseline: Not Selected	PT-2	PT-2	PT-2	PT-2
PT-2	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, updating and/or sharing 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 (3) What is consistent with applicable laws, regulations and contractual obligations.	5	NIST SP 800-53B R5 Baseline: Not Selected	PT-2	PT-2	PT-2	PT-2
PT-2	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 from minors without appropriate parental or legal guardian consent.	5	NIST SP 800-53B R5 Baseline: Not Selected	PT-2	PT-2	PT-2	PT-2
PT-2(1)	Authority to Process Personally Identifiable Information | Data Tagging	Attach data tags containing [Assignment: organization-defined authorized processing] to [Assignment: organization-defined elements of personally identifiable information].	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	NIST SP 800-53B R5 Baseline: Not Selected				
PT-2(2)	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, based on updated data subject	5	NIST SP 800-53B R5 Baseline: Not Selected				
PT-3	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:	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	5	NIST SP 800-53B R5 Baseline: Not Selected	PT-3	PT-3	PT-3	PT-3

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)	Low	Mod	High	Privacy
PT-3	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:	Functional	Intersects With	Purpose Specification	PRI-02.1	Mechanisms exist to ensure the data privacy notice identifies the purpose(s) for which Personal Data (PD) is collected, received, processed, stored, transmitted, shared.	5	NIST SP 800-53B R5 Baseline: Not Selected	PT-3	PT-3	PT-3	PT-3
PT-3(1)	Personally Identifiable Information Processing Purposes | Data Tagging	Attach data tags containing the following purposes to [Assignment: organization-defined elements of personally identifiable information]: [Assignment: organization-defined processing purposes].	Functional	Intersects With	Data Tagging	PRI-11	Mechanisms exist to issue data modeling guidelines to support tagging of sensitive/regulated data.	5	NIST SP 800-53B R5 Baseline: Not Selected	PT-3(1)	PT-3(1)	PT-3(1)	PT-3(1)
PT-3(1)	Personally Identifiable Information Processing Purposes | Data Tagging	Attach data tags containing the following purposes to [Assignment: organization-defined elements of personally identifiable information]: [Assignment: organization-defined processing purposes].	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	NIST SP 800-53B R5 Baseline: Not Selected	PT-3(1)	PT-3(1)	PT-3(1)	PT-3(1)
PT-3(2)	Personally Identifiable Information Processing Purposes |	Track processing purposes of personally identifiable information using [Assignment: organization-defined automated mechanisms].	Functional	Intersects With	Automation	PRI-10.1	Automated mechanisms exist to support the evaluation of data quality across the information lifecycle.	5	NIST SP 800-53B R5 Baseline: Not Selected	PT-3(2)	PT-3(2)	PT-3(2)	PT-3(2)
PT-3(2)	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, based on updated data subject	5	NIST SP 800-53B R5 Baseline: Not Selected	PT-3(2)	PT-3(2)	PT-3(2)	PT-3(2)
PT-4	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, processing, storage, sharing, updating and disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (1) Plain language to illustrate the potential data privacy risks of the authorization; (2) A means for users to decline the authorization; and (3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	10	NIST SP 800-53B R5 Baseline: Not Selected				PT-4
PT-4(1)	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, update and/or share selected attributes of their Personal	10	NIST SP 800-53B R5 Baseline: Not Selected				
PT-4(2)	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 process, store and/or share 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 has passed since an individual gave	5	NIST SP 800-53B R5 Baseline: Not Selected				
PT-4(3)	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, transmit, update and/or share their Personal Data (PD).	10	NIST SP 800-53B R5 Baseline: Not Selected				
PT-5	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 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 (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	5	NIST SP 800-53B R5 Baseline: Not Selected				PT-5
PT-5(1)	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 process, store and/or share 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 has passed since an individual gave	5	NIST SP 800-53B R5 Baseline: Not Selected				
PT-5(2)	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	NIST SP 800-53B R5 Baseline: Not Selected				PT-5(2)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)	Low	Mod	High	Privacy
PT-6	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	NIST SP 800-53B R5 Baseline: Not Selected				PT-6
PT-6(1)	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	NIST SP 800-53B R5 Baseline: Not Selected				PT-6(1)
PT-6(2)	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	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	NIST SP 800-53B R5 Baseline: Not Selected				PT-6(2)
PT-7	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, updating and/or sharing 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 (3) What is consistent with applicable laws, regulations and contractual obligations.	5	NIST SP 800-53B R5 Baseline: Not Selected	PT-7	PT-7	PT-7	PT-7
PT-7	Specific Categories of Personally Identifiable Information	Apply [Assignment: organization-defined processing conditions] for specific categories of personally identifiable information.	Functional	Intersects With	Personal Data Categories	PRI-05.7	Mechanisms exist to define and implement data handling and protection requirements for specific categories of sensitive Personal Data	5	NIST SP 800-53B R5 Baseline: Not Selected	PT-7	PT-7	PT-7	PT-7
PT-7(1)	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 Categories	PRI-05.7	Mechanisms exist to define and implement data handling and protection requirements for specific categories of sensitive Personal Data (PD).	5	NIST SP 800-53B R5 Baseline: Not Selected				PT-7(1)
PT-7(2)	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 Categories	PRI-05.7	Mechanisms exist to define and implement data handling and protection requirements for specific categories of sensitive Personal Data (PD).	5	NIST SP 800-53B R5 Baseline: Not Selected				PT-7(2)
PT-8	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	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	NIST SP 800-53B R5 Baseline: Not Selected				PT-8
RA-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] risk assessment policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 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:	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	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 continuing suitability, adequacy and effectiveness.	5	NIST SP 800-53B R5 Baseline: Low	RA-1	RA-1	RA-1	RA-1
RA-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] risk assessment policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 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:	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	NIST SP 800-53B R5 Baseline: Low	RA-1	RA-1	RA-1	RA-1
RA-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] risk assessment policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 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:	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	NIST SP 800-53B R5 Baseline: Low	RA-1	RA-1	RA-1	RA-1

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)	Low	Mod	High	Privacy
RA-2	Security Categorization	a. Categorize the system and information it processes, stores, and transmits;b. Document the security categorization results, including supporting rationale, in the security plan for the system; 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 systems and data 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	NIST SP 800-53B R5 Baseline: Low	RA-2	RA-2	RA-2	
RA-2(1)	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 systems, applications and/or services to prevent potential disruptions.	10	NIST SP 800-53B R5 Baseline: Not Selected				
RA-3	Risk Assessment	a. Conduct a risk assessment, including:1. Identifying threats to and vulnerabilities in the system;2. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; 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	Functional	Intersects With	Functional Review Of Cybersecurity & Data Protection Controls	CPL-03.2	Mechanisms exist to regularly review technology assets for adherence to the organization's cybersecurity & data protection policies and standards.	5	NIST SP 800-53B R5 Baseline: Low	RA-3	RA-3	RA-3	RA-3
RA-3	Risk Assessment	a. Conduct a risk assessment, including:1. Identifying threats to and vulnerabilities in the system;2. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; 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	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 systems and data.	5	NIST SP 800-53B R5 Baseline: Low	RA-3	RA-3	RA-3	RA-3
RA-3(1)	Risk Assessment | Supply Chain Risk Assessment	a. Assess supply chain risks associated with [Assignment: organization-defined systems, system components, and system services]; 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	Functional	Equal	Supply Chain Risk Assessment	RSK-09.1	Mechanisms exist to periodically assess supply chain risks associated with systems, system components and services.	10	NIST SP 800-53B R5 Baseline: Low	RA-3(1)	RA-3(1)	RA-3(1)	
RA-3(2)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
RA-3(3)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
RA-3(4)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
RA-4	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
RA-5	Vulnerability Monitoring and Scanning	a. Monitor and scan for vulnerabilities in the system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system are identified and reported;b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:1. Enumerating platforms, software flaws, and improper configurations;2. Formatting checklists and test procedures; 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	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	NIST SP 800-53B R5 Baseline: Low	RA-5	RA-5	RA-5	RA-5
RA-5	Vulnerability Monitoring and Scanning	a. Monitor and scan for vulnerabilities in the system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system are identified and reported;b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:1. Enumerating platforms, software flaws, and improper configurations;2. Formatting checklists and test procedures; 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	Functional	Intersects With	Update Tool Capability	VPM-06.1	Mechanisms exist to update vulnerability scanning tools.	5	NIST SP 800-53B R5 Baseline: Low	RA-5	RA-5	RA-5	RA-5
RA-5(1)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
RA-5(2)	Vulnerability Monitoring and Scanning | Update Vulnerabilities to Be	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	NIST SP 800-53B R5 Baseline: Low	RA-5(2)	RA-5(2)	RA-5(2)	
RA-5(3)	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	10	NIST SP 800-53B R5 Baseline: 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 (optional)	Notes (optional)	Low	Mod	High	Privacy
RA-5(4)	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 remediated non-compliant systems.	10	NIST SP 800-53B R5 Baseline: High			RA-5(4)	
RA-5(5)	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	NIST SP 800-53B R5 Baseline: Moderate		RA-5(5)	RA-5(5)	
RA-5(6)	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	NIST SP 800-53B R5 Baseline: Not Selected				
RA-5(7)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
RA-5(8)	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	NIST SP 800-53B R5 Baseline: Not Selected				
RA-5(9)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
RA-5(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	10	NIST SP 800-53B R5 Baseline: Not Selected				
RA-5(11)	Vulnerability Monitoring and Scanning | Public Disclosure Program	Establish a public reporting channel for receiving reports of vulnerabilities in organizational systems and system components.	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 products and services that receives unsolicited input from the public about vulnerabilities in organizational systems, services and processes.	10	NIST SP 800-53B R5 Baseline: Low	RA-5(11)	RA-5(11)	RA-5(11)	
RA-6	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	NIST SP 800-53B R5 Baseline: Not Selected				
RA-7	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	Mechanisms exist to respond to findings from cybersecurity & data privacy assessments, incidents and audits to ensure proper remediation has been performed.	10	NIST SP 800-53B R5 Baseline: Low	RA-7	RA-7	RA-7	RA-7
RA-8	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 systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	NIST SP 800-53B R5 Baseline: Not Selected				RA-8
RA-9	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 systems, components and services using a supply chain risk assessment process relative to their importance in supporting the delivery of high-	5	NIST SP 800-53B R5 Baseline: Moderate	RA-9	RA-9	RA-9	RA-9
RA-9	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	TDA-06.1	Mechanisms exist to require the developer of the system, system component or service to perform a criticality analysis at organization-defined decision points in the Secure Development Life Cycle (SDLC).	5	NIST SP 800-53B R5 Baseline: Moderate	RA-9	RA-9	RA-9	RA-9
RA-9	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	Cybersecurity & Data Privacy Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical systems, system components or services at pre-defined decision points in the Secure Development Life Cycle (SDLC).	5	NIST SP 800-53B R5 Baseline: Moderate	RA-9	RA-9	RA-9	RA-9
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	NIST SP 800-53B R5 Baseline: Not Selected				
SA-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and services acquisition policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 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	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	NIST SP 800-53B R5 Baseline: Low	SA-1	SA-1	SA-1	SA-1
SA-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and services acquisition policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 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	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	NIST SP 800-53B R5 Baseline: Low	SA-1	SA-1	SA-1	SA-1

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)	Low	Mod	High	Privacy
SA-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and services acquisition policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 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	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	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 continuing suitability, adequacy and effectiveness.	5	NIST SP 800-53B R5 Baseline: Low	SA-1	SA-1	SA-1	SA-1
SA-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and services acquisition policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 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	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5	NIST SP 800-53B R5 Baseline: Low	SA-1	SA-1	SA-1	SA-1
SA-2	Allocation of Resources	a. Determine the high-level information security and privacy requirements for the system or system service in mission and business process planning;b. Determine, document, and allocate the resources required to protect the system or system service as part of the organizational capital planning and investment control process; 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 privacy requirements within business process planning for projects / initiatives.	10	NIST SP 800-53B R5 Baseline: Low	SA-2	SA-2	SA-2	SA-2
SA-3	System Development Life Cycle	a. Acquire, develop, and manage the system using [Assignment: organization-defined system development life cycle] that incorporates information security and privacy considerations;b. Define and document information security and privacy roles and responsibilities throughout the system development life cycle;c. Identify individuals having information security and privacy roles and responsibilities; andd. Integrate the organizational information security and privacy risk management process into system development life	Functional	Intersects With	Technology Lifecycle Management	SEA-07.1	Mechanisms exist to manage the usable lifecycles of technology assets.	5	NIST SP 800-53B R5 Baseline: Low	SA-3	SA-3	SA-3	SA-3
SA-3	System Development Life Cycle	a. Acquire, develop, and manage the system using [Assignment: organization-defined system development life cycle] that incorporates information security and privacy considerations;b. Define and document information security and privacy roles and responsibilities throughout the system development life cycle;c. Identify individuals having information security and privacy roles and responsibilities; andd. Integrate the organizational information security and privacy risk management process into system development life	Functional	Intersects With	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to systems within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5	NIST SP 800-53B R5 Baseline: Low	SA-3	SA-3	SA-3	SA-3
SA-3(1)	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.	5	NIST SP 800-53B R5 Baseline: Not Selected	SA-3(1)	SA-3(1)	SA-3(1)	SA-3(1)
SA-3(1)	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 systems within the Secure Development Life Cycle (SDLC) are controlled through formal change	5	NIST SP 800-53B R5 Baseline: Not Selected	SA-3(1)	SA-3(1)	SA-3(1)	SA-3(1)
SA-3(1)	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	NIST SP 800-53B R5 Baseline: Not Selected	SA-3(1)	SA-3(1)	SA-3(1)	SA-3(1)
SA-3(2)	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	NIST SP 800-53B R5 Baseline: Not Selected				
SA-3(3)	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.	5	NIST SP 800-53B R5 Baseline: Not Selected	SA-3(3)	SA-3(3)	SA-3(3)	SA-3(3)
SA-3(3)	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 information system component and service refreshes are obtained from trusted sources.	5	NIST SP 800-53B R5 Baseline: Not Selected	SA-3(3)	SA-3(3)	SA-3(3)	SA-3(3)
SA-4	Acquisition Process	Include the following requirements, descriptions, and criteria, explicitly or by reference, using [Selection (one or more): standardized contract language; [Assignment: organization-defined contract language]] in the acquisition contract for the system, system component, or system service:a. Security and privacy functional requirements;b. Strength of mechanism requirements;c. Security and privacy assurance requirements;d. Controls needed to satisfy the security and privacy requirements.e. Security and privacy documentation requirements;f. Requirements for protecting security and privacy documentation;g. Description of the system development environment and environment in which the system is intended to operate;h. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; andi. Acceptance	Functional	Intersects With	Minimum Viable Product (MVP) Security Requirements	TDA-02	Mechanisms exist to design, develop and produce products and/or services 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	NIST SP 800-53B R5 Baseline: Low	SA-4	SA-4	SA-4	SA-4
SA-4	Acquisition Process	Include the following requirements, descriptions, and criteria, explicitly or by reference, using [Selection (one or more): standardized contract language; [Assignment: organization-defined contract language]] in the acquisition contract for the system, system component, or system service:a. Security and privacy functional requirements;b. Strength of mechanism requirements;c. Security and privacy assurance requirements;d. Controls needed to satisfy the security and privacy requirements.e. Security and privacy documentation requirements;f. Requirements for protecting security and privacy documentation;g. Description of the system development environment and environment in which the system is intended to operate;h. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; andi. Acceptance	Functional	Intersects With	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	NIST SP 800-53B R5 Baseline: Low	SA-4	SA-4	SA-4	SA-4

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)	Low	Mod	High	Privacy
SA-4	Acquisition Process	Include the following requirements, descriptions, and criteria, explicitly or by reference, using [Selection (one or more): standardized contract language; [Assignment: organization-defined contract language]] in the acquisition contract for the system, system component, or system service:a. Security and privacy functional requirements;b. Strength of mechanism requirements;c. Security and privacy assurance requirements;d. Controls needed to satisfy the security and privacy requirements.e. Security and privacy documentation requirements;f. Requirements for protecting security and privacy documentation;g. Description of the system development environment and environment in which the system is intended to operate;h. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; andi. Acceptance	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	NIST SP 800-53B R5 Baseline: Low	SA-4	SA-4	SA-4	SA-4
SA-4	Acquisition Process	Include the following requirements, descriptions, and criteria, explicitly or by reference, using [Selection (one or more): standardized contract language; [Assignment: organization-defined contract language]] in the acquisition contract for the system, system component, or system service:a. Security and privacy functional requirements;b. Strength of mechanism requirements;c. Security and privacy assurance requirements;d. Controls needed to satisfy the security and privacy requirements.e. Security and privacy documentation requirements;f. Requirements for protecting security and privacy documentation;g. Description of the system development environment and environment in which the system is intended to operate;h. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; andi. Acceptance	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 information, systems and processes that are in scope by the third-party.	5	NIST SP 800-53B R5 Baseline: Low	SA-4	SA-4	SA-4	SA-4
SA-4(1)	Acquisition Process | Functional Properties of Controls	Require the developer of the system, system component, or system service to provide a description of the functional properties of the controls to be implemented.	Functional	Intersects With	Functional Properties	TDA-04.1	Mechanisms exist to require software developers to provide information describing the functional properties of the security controls to be utilized within systems, system components or services in sufficient detail to permit analysis and testing of the	5	NIST SP 800-53B R5 Baseline: Moderate	SA-4(1)	SA-4(1)	SA-4(1)	SA-4(1)
SA-4(1)	Acquisition Process | Functional Properties of Controls	Require the developer of the system, system component, or system service to provide a description of the functional properties of the controls to be implemented.	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	NIST SP 800-53B R5 Baseline: Moderate	SA-4(1)	SA-4(1)	SA-4(1)	SA-4(1)
SA-4(2)	Acquisition Process | Design and Implementation Information for Controls	Require the developer of the system, system component, or system service to provide design and implementation information for the controls that includes: [Selection (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; [Assignment: organization-defined design and implementation information]] at [Assignment: organization-defined level of detail].	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	NIST SP 800-53B R5 Baseline: Moderate	SA-4(2)	SA-4(2)	SA-4(2)	SA-4(2)
SA-4(2)	Acquisition Process | Design and Implementation Information for Controls	Require the developer of the system, system component, or system service to provide design and implementation information for the controls that includes: [Selection (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; [Assignment: organization-defined design and implementation information]] at [Assignment: organization-defined level of	Functional	Intersects With	Access to Program Source Code	TDA-20	Mechanisms exist to limit privileges to change software resident within software libraries.	5	NIST SP 800-53B R5 Baseline: Moderate	SA-4(2)	SA-4(2)	SA-4(2)	SA-4(2)
SA-4(2)	Acquisition Process | Design and Implementation Information for Controls	Require the developer of the system, system component, or system service to provide design and implementation information for the controls that includes: [Selection (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; [Assignment: organization-defined design and implementation information]] at [Assignment: organization-defined level of	Functional	Intersects With	Functional Properties	TDA-04.1	Mechanisms exist to require software developers to provide information describing the functional properties of the security controls to be utilized within systems, system components or services in sufficient detail to permit analysis and testing of the	5	NIST SP 800-53B R5 Baseline: Moderate	SA-4(2)	SA-4(2)	SA-4(2)	SA-4(2)
SA-4(3)	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	NIST SP 800-53B R5 Baseline: Not Selected	SA-4(3)	SA-4(3)	SA-4(3)	SA-4(3)
SA-4(3)	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	NIST SP 800-53B R5 Baseline: Not Selected	SA-4(3)	SA-4(3)	SA-4(3)	SA-4(3)
SA-4(4)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SA-4(5)	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 system, component, or service with a pre-established, secure configuration implemented; and (2) Use the pre-established, secure configuration as the default for any subsequent system, component, or	10	NIST SP 800-53B R5 Baseline: High			SA-4(5)	
SA-4(6)	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	Functional	Equal	Commercial Off-The-Shelf (COTS) Security Solutions	TDA-03	Mechanisms exist to utilize only Commercial Off-the-Shelf (COTS) security products.	10	NIST SP 800-53B R5 Baseline: Not Selected				
SA-4(7)	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	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	NIST SP 800-53B R5 Baseline: Not Selected				
SA-4(8)	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 systems, system components or services to produce a plan for the continuous monitoring of cybersecurity & data privacy control effectiveness.	10	NIST SP 800-53B R5 Baseline: 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 (optional)	Notes (optional)	Low	Mod	High	Privacy
SA-4(9)	Acquisition Process | Functions, Ports, Protocols, and Services in Use	Require the developer of the system, system component, or system service to identify the functions, ports, protocols, and services intended for organizational use.	Functional	Equal	Ports, Protocols & Services In Use	TDA-02.1	Mechanisms exist to require the developers of systems, system components or services to identify early in the Secure Development Life Cycle (SDLC), the functions, ports, protocols and services intended for	10	NIST SP 800-53B R5 Baseline: Moderate		SA-4(9)	SA-4(9)	
SA-4(10)	Acquisition Process | Use of Approved PIV Products	Employ only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational systems.	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-	5	NIST SP 800-53B R5 Baseline: Low	SA-4(10)	SA-4(10)	SA-4(10)	
SA-4(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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SA-4(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, updates and/or disposes of PD.	5	NIST SP 800-53B R5 Baseline: Not Selected	SA-4(12)	SA-4(12)	SA-4(12)	SA-4(12)
SA-4(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	NIST SP 800-53B R5 Baseline: Not Selected	SA-4(12)	SA-4(12)	SA-4(12)	SA-4(12)
SA-4(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	NIST SP 800-53B R5 Baseline: Not Selected	SA-4(12)	SA-4(12)	SA-4(12)	SA-4(12)
SA-5	System Documentation	a. Obtain or develop administrator documentation for the system, system component, or system service that describes:1. Secure configuration, installation, and operation of the system, component, or service;2. Effective use and maintenance of security and privacy functions and mechanisms; 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	Functional	Intersects With	Documentation Requirements	TDA-04	Mechanisms exist to obtain, protect and distribute administrator documentation for systems that describe: (1) Secure configuration, installation and operation of the system; (2) Effective use and maintenance of security features/functions; and (3) Known vulnerabilities regarding configuration and use of administrative (e.g., privileged) functions.	5	NIST SP 800-53B R5 Baseline: Low	SA-5	SA-5	SA-5	SA-5
SA-5	System Documentation	a. Obtain or develop administrator documentation for the system, system component, or system service that describes:1. Secure configuration, installation, and operation of the system, component, or service;2. Effective use and maintenance of security and privacy functions and mechanisms; 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	Functional	Intersects With	Asset Scope Classification	AST-04.1	Mechanisms exist to determine cybersecurity & data privacy control applicability by identifying, assigning and documenting the appropriate asset scope categorization for all systems, applications, services and personnel (internal and third-parties).	5	NIST SP 800-53B R5 Baseline: Low	SA-5	SA-5	SA-5	SA-5
SA-5(1)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SA-5(2)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SA-5(3)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SA-5(4)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SA-5(5)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SA-6	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SA-7	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SA-8	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	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	NIST SP 800-53B R5 Baseline: Low	SA-8	SA-8	SA-8	SA-8
SA-8	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 cybersecurity & data privacy practices in the specification, design, development, implementation and modification of	5	NIST SP 800-53B R5 Baseline: Low	SA-8	SA-8	SA-8	SA-8
SA-8(1)	Security and Privacy Engineering Principles | Clear Abstractions	Implement the security design principle of clear abstractions.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SA-8(2)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SA-8(3)	Security and Privacy Engineering Principles | Modularity and	Implement the security design principles of modularity and layering in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SA-8(4)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SA-8(5)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SA-8(6)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SA-8(7)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SA-8(8)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: 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 (optional)	Notes (optional)	Low	Mod	High	Privacy
SA-8(9)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SA-8(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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SA-8(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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SA-8(12)	Security and 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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SA-8(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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SA-8(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	NIST SP 800-53B R5 Baseline: Not Selected				
SA-8(15)	Security and Privacy Engineering Principles | Predicate Permission	Implement the security design principle of predicate permission in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SA-8(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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SA-8(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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SA-8(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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SA-8(19)	Security and 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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SA-8(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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SA-8(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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SA-8(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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SA-8(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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SA-8(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	Mechanisms exist to enable systems to fail to an organization-defined known-state for types of failures, preserving system state information	10	NIST SP 800-53B R5 Baseline: Not Selected				
SA-8(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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SA-8(26)	Security and 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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SA-8(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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SA-8(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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SA-8(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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SA-8(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 systems within the Secure Development Life Cycle (SDLC) are controlled through formal change	5	NIST SP 800-53B R5 Baseline: Not Selected	SA-8(30)	SA-8(30)	SA-8(30)	SA-8(30)
SA-8(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.	5	NIST SP 800-53B R5 Baseline: Not Selected	SA-8(30)	SA-8(30)	SA-8(30)	SA-8(30)
SA-8(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	NIST SP 800-53B R5 Baseline: Not Selected	SA-8(31)	SA-8(31)	SA-8(31)	SA-8(31)
SA-8(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 cybersecurity and/or data privacy controls following implemented changes to ensure applicable controls operate as designed.	5	NIST SP 800-53B R5 Baseline: Not Selected	SA-8(31)	SA-8(31)	SA-8(31)	SA-8(31)
SA-8(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	NIST SP 800-53B R5 Baseline: Not Selected	SA-8(31)	SA-8(31)	SA-8(31)	SA-8(31)
SA-8(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	NIST SP 800-53B R5 Baseline: Not Selected				
SA-8(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	NIST SP 800-53B R5 Baseline: Not Selected	SA-8(33)	SA-8(33)	SA-8(33)	SA-8(33)
SA-8(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	NIST SP 800-53B R5 Baseline: Not Selected	SA-8(33)	SA-8(33)	SA-8(33)	SA-8(33)
SA-8(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	NIST SP 800-53B R5 Baseline: Not Selected	SA-8(33)	SA-8(33)	SA-8(33)	SA-8(33)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)	Low	Mod	High	Privacy
SA-9	External System Services	a. Require that providers of external system services comply with organizational security and privacy requirements and employ the following controls: [Assignment: organization-defined controls];b. Define and document organizational oversight and user roles and responsibilities with regard to external system services; 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	Functional	Equal	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's systems and data.	10	NIST SP 800-53B R5 Baseline: Low	SA-9	SA-9	SA-9	SA-9
SA-9(1)	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 services.	10	NIST SP 800-53B R5 Baseline: Not Selected				
SA-9(2)	External System Services | Identification of Functions, Ports, Protocols, and Services	Require providers of the following external system services to identify the functions, ports, protocols, and other services required for the use of such services: [Assignment: organization-defined external system services].	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 processes and technologies.	10	NIST SP 800-53B R5 Baseline: Moderate		SA-9(2)	SA-9(2)	
SA-9(3)	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 systems, system components and services, including documenting selected mitigating actions and monitoring performance against	5	NIST SP 800-53B R5 Baseline: Not Selected				
SA-9(3)	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 systems, components and services using a supply chain risk assessment process relative to their importance in supporting the delivery of high-	5	NIST SP 800-53B R5 Baseline: Not Selected				
SA-9(3)	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 the services and product supply chains; and (2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	5	NIST SP 800-53B R5 Baseline: Not Selected				
SA-9(3)	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 Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and	5	NIST SP 800-53B R5 Baseline: Not Selected				
SA-9(3)	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 cybersecurity & data privacy controls between internal stakeholders and External Service Providers (ESPs).	5	NIST SP 800-53B R5 Baseline: Not Selected				
SA-9(3)	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	Functional	Intersects With	Break Clauses	TPM-05.7	Mechanisms exist to include "break clauses" within contracts for failure to meet contract criteria for cybersecurity and/or data privacy controls.	5	NIST SP 800-53B R5 Baseline: Not Selected				
SA-9(4)	External System Services | Consistent Interests of Consumers and	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	NIST SP 800-53B R5 Baseline: Not Selected				
SA-9(5)	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	NIST SP 800-53B R5 Baseline: Not Selected	SA-9(5)	SA-9(5)	SA-9(5)	SA-9(5)
SA-9(5)	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	NIST SP 800-53B R5 Baseline: Not Selected	SA-9(5)	SA-9(5)	SA-9(5)	SA-9(5)
SA-9(5)	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-	5	NIST SP 800-53B R5 Baseline: Not Selected	SA-9(5)	SA-9(5)	SA-9(5)	SA-9(5)
SA-9(6)	External System Services | Organization-controlled	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	NIST SP 800-53B R5 Baseline: Not Selected				
SA-9(7)	External System Services | Organization-controlled Integrity	Provide the capability to check the integrity of information while it resides in the external system.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SA-9(8)	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-	5	NIST SP 800-53B R5 Baseline: Not Selected	SA-9(8)	SA-9(8)	SA-9(8)	SA-9(8)
SA-9(8)	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	NIST SP 800-53B R5 Baseline: Not Selected	SA-9(8)	SA-9(8)	SA-9(8)	SA-9(8)
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	NIST SP 800-53B R5 Baseline: Moderate		SA-10	SA-10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)	Low	Mod	High	Privacy
SA-10(1)	Developer Configuration Management | Software and Firmware Integrity	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 developer of systems, system components or services to enable integrity verification of software and firmware components.	10	NIST SP 800-53B R5 Baseline: Not Selected				
SA-10(2)	Developer Configuration Management | Alternative Configuration Management	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SA-10(3)	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 developer of systems, system components or services to enable integrity verification of hardware components.	10	NIST SP 800-53B R5 Baseline: Not Selected				
SA-10(4)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SA-10(5)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SA-10(6)	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	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SA-10(7)	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	Cybersecurity & Data Privacy Representatives For Product Changes	TDA-02.7	Mechanisms exist to include appropriate cybersecurity & data privacy representatives in the product feature and/or functionality change control review process.	10	NIST SP 800-53B R5 Baseline: 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	Cybersecurity & Data Privacy Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with cybersecurity & data privacy 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 security testing and evaluation process; and (3) Document the results of the security testing/evaluation and flaw remediation processes.	10	NIST SP 800-53B R5 Baseline: Moderate		SA-11	SA-11	SA-11
SA-11(1)	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 systems, system components or services to employ static code analysis tools to identify and remediate common flaws and document the results of the analysis.	10	NIST SP 800-53B R5 Baseline: Not Selected				
SA-11(2)	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 Analysis & Flaw F	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	NIST SP 800-53B R5 Baseline: Not Selected	SA-11(2)	SA-11(2)	SA-11(2)	SA-11(2)
SA-11(2)	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	NIST SP 800-53B R5 Baseline: Not Selected	SA-11(2)	SA-11(2)	SA-11(2)	SA-11(2)
SA-11(3)	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	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SA-11(4)	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 systems, system components or services to employ a manual code review process to identify and remediate unique flaws that require knowledge of the application's requirements and	10	NIST SP 800-53B R5 Baseline: Not Selected				
SA-11(5)	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	NIST SP 800-53B R5 Baseline: Not Selected	SA-11(5)	SA-11(5)	SA-11(5)	SA-11(5)
SA-11(5)	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 applications and services.	5	NIST SP 800-53B R5 Baseline: Not Selected	SA-11(5)	SA-11(5)	SA-11(5)	SA-11(5)
SA-11(5)	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	Cybersecurity & Data Privacy Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with cybersecurity & data privacy 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 security testing and evaluation process; and (3) Document the results of the security testing/evaluation and flaw remediation processes.	5	NIST SP 800-53B R5 Baseline: Not Selected	SA-11(5)	SA-11(5)	SA-11(5)	SA-11(5)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)	Low	Mod	High	Privacy
SA-11(5)	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	5	NIST SP 800-53B R5 Baseline: Not Selected	SA-11(5)	SA-11(5)	SA-11(5)	SA-11(5)
SA-11(5)	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 systems and web applications.	5	NIST SP 800-53B R5 Baseline: Not Selected	SA-11(5)	SA-11(5)	SA-11(5)	SA-11(5)
SA-11(6)	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	Cybersecurity & Data Privacy Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with cybersecurity & data privacy 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 security testing and evaluation process; and (3) Document the results of the security testing/evaluation and flaw remediation processes.	5	NIST SP 800-53B R5 Baseline: Not Selected	SA-11(6)	SA-11(6)	SA-11(6)	SA-11(6)
SA-11(6)	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	NIST SP 800-53B R5 Baseline: Not Selected	SA-11(6)	SA-11(6)	SA-11(6)	SA-11(6)
SA-11(7)	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	NIST SP 800-53B R5 Baseline: Not Selected	SA-11(7)	SA-11(7)	SA-11(7)	SA-11(7)
SA-11(7)	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	Cybersecurity & Data Privacy Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with cybersecurity & data privacy 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 security testing and evaluation process; and (3) Document the results of the security testing/evaluation and flaw remediation processes.	5	NIST SP 800-53B R5 Baseline: Not Selected	SA-11(7)	SA-11(7)	SA-11(7)	SA-11(7)
SA-11(8)	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 systems, system components or services to employ dynamic code analysis tools to identify and remediate common flaws and document the results of the	10	NIST SP 800-53B R5 Baseline: Not Selected				
SA-11(9)	Developer Testing and Evaluation | Interactive Application Security	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SA-12	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SA-12(1)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SA-12(2)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SA-12(3)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SA-12(4)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SA-12(5)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SA-12(6)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SA-12(7)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SA-12(8)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SA-12(9)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SA-12(10)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SA-12(11)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SA-12(12)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SA-12(13)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SA-12(14)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SA-12(15)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SA-13	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SA-14	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SA-14(1)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	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	Functional	Equal	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	10	NIST SP 800-53B R5 Baseline: Moderate		SA-15	SA-15	
SA-15(1)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SA-15(2)	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	Plan of Action & Milestones (POA&M)	IAO-05	Mechanisms exist to generate a Plan of Action and Milestones (POA&M), or similar risk register, 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.	10	NIST SP 800-53B R5 Baseline: Not Selected				
SA-15(3)	Development Process, Standards, and Tools | Criticality Analysis	Require the developer of the system, system component, or system service to perform a criticality analysis:a. At the following decision points in the system development life cycle: [Assignment: organization-defined decision points in the system development life cycle]; andb. At the following level of rigor: [Assignment: organization-defined breadth and depth of	Functional	Equal	Criticality Analysis	TDA-06.1	Mechanisms exist to require the developer of the system, system component or service to perform a criticality analysis at organization-defined decision points in the Secure Development Life Cycle (SDLC).	10	NIST SP 800-53B R5 Baseline: Moderate		SA-15(3)	SA-15(3)	
SA-15(4)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	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 (optional)	Notes (optional)	Low	Mod	High	Privacy
SA-15(5)	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	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	NIST SP 800-53B R5 Baseline: Not Selected	SA-15(5)	SA-15(5)	SA-15(5)	SA-15(5)
SA-15(5)	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 cybersecurity & data privacy practices in the specification, design, development, implementation and modification of	5	NIST SP 800-53B R5 Baseline: Not Selected	SA-15(5)	SA-15(5)	SA-15(5)	SA-15(5)
SA-15(6)	Development Process, Standards, and Tools | Continuous	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SA-15(7)	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	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SA-15(8)	Development Process, Standards, and Tools | Reuse of Threat and Vulnerability	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	NIST SP 800-53B R5 Baseline: Not Selected				
SA-15(9)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SA-15(10)	Development Process, Standards, and Tools | Incident	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: 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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: 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	NIST SP 800-53B R5 Baseline: 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 systems, system components or services to provide training on the correct use and operation of the system, system component or service.	10	NIST SP 800-53B R5 Baseline: High			SA-16	
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 systems, system components or services 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 controls among physical and logical components; and (3) Expresses how individual security functions, mechanisms and services work together to provide required security capabilities and a unified	10	NIST SP 800-53B R5 Baseline: High			SA-17	
SA-17(1)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SA-17(2)	Developer Security and Privacy Architecture and Design | Security-	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	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SA-17(3)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SA-17(4)	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	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SA-17(5)	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	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: 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 (optional)	Notes (optional)	Low	Mod	High	Privacy
SA-17(6)	Developer Security and Privacy Architecture and Design | Structure for	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SA-17(7)	Developer Security and Privacy Architecture and Design | Structure for	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SA-17(8)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SA-17(9)	Developer Security and Privacy Architecture and Design | Design	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SA-18	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SA-18(1)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SA-18(2)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SA-19	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SA-19(1)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SA-19(2)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SA-19(3)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SA-19(4)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	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	NIST SP 800-53B R5 Baseline: 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	Functional	Equal	Developer Screening	TDA-13	Mechanisms exist to ensure that the developers of systems, applications and/or services have the requisite skillset and appropriate access authorizations.	10	NIST SP 800-53B R5 Baseline: High			SA-21	
SA-21(1)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
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 Systems	TDA-17	Mechanisms exist to prevent unsupported systems by: (1) Replacing systems 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 system components required to satisfy mission/business needs.	5	NIST SP 800-53B R5 Baseline: Low	SA-22	SA-22	SA-22	SA-22
SA-22	Unsupported System Components	a. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; 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	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 system components.	5	NIST SP 800-53B R5 Baseline: Low	SA-22	SA-22	SA-22	SA-22
SA-22(1)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	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	5	NIST SP 800-53B R5 Baseline: Not Selected	SA-23	SA-23	SA-23	SA-23
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 products and/or services 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 contractual obligations.	5	NIST SP 800-53B R5 Baseline: Not Selected	SA-23	SA-23	SA-23	SA-23
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	NIST SP 800-53B R5 Baseline: Not Selected	SA-23	SA-23	SA-23	SA-23
SC-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and communications protection policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 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	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	NIST SP 800-53B R5 Baseline: Low	SC-1	SC-1	SC-1	SC-1
SC-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and communications protection policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 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	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	NIST SP 800-53B R5 Baseline: Low	SC-1	SC-1	SC-1	SC-1

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)	Low	Mod	High	Privacy
SC-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and communications protection policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 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	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity & data privacy practices in the specification, design, development, implementation and modification of systems and services.	10	NIST SP 800-53B R5 Baseline: Low	SC-1	SC-1	SC-1	SC-1
SC-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and communications protection policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 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	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	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 continuing suitability, adequacy and effectiveness.	5	NIST SP 800-53B R5 Baseline: Low	SC-1	SC-1	SC-1	SC-1
SC-2	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	NIST SP 800-53B R5 Baseline: Moderate		SC-2	SC-2	
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.	Functional	Equal	Application Partitioning	SEA-03.2	Mechanisms exist to separate user functionality from system management functionality.	10	NIST SP 800-53B R5 Baseline: Not Selected				
SC-2(2)	Separation of System and User Functionality | Disassociability	Store state information from applications and software separately.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SC-3	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	NIST SP 800-53B R5 Baseline: High	SC-3	SC-3	SC-3	SC-3
SC-3	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	5	NIST SP 800-53B R5 Baseline: High	SC-3	SC-3	SC-3	SC-3
SC-3(1)	Security Function Isolation | Hardware Separation	Employ hardware separation mechanisms to implement security function isolation.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SC-3(2)	Security Function Isolation | Access and Flow Control	Isolate security functions enforcing access and information flow control from nonsecurity functions and from other security functions.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SC-3(3)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SC-3(4)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SC-3(5)	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	NIST SP 800-53B R5 Baseline: Not Selected				
SC-4	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	NIST SP 800-53B R5 Baseline: Moderate		SC-4	SC-4	
SC-4(1)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SC-4(2)	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	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SC-5	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 systems that are susceptible to Denial of Service (DoS) attacks to limit and prioritize the use of resources.	5	NIST SP 800-53B R5 Baseline: Low	SC-5	SC-5	SC-5	SC-5
SC-5	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	NIST SP 800-53B R5 Baseline: Low	SC-5	SC-5	SC-5	SC-5
SC-5	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	NIST SP 800-53B R5 Baseline: Low	SC-5	SC-5	SC-5	SC-5
SC-5	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	NIST SP 800-53B R5 Baseline: Low	SC-5	SC-5	SC-5	SC-5
SC-5(1)	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 systems that are susceptible to Denial of Service (DoS) attacks to limit and prioritize the use of resources.	5	NIST SP 800-53B R5 Baseline: Not Selected				
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 attacks.	Functional	Intersects With	Resource Priority	CAP-02	Mechanisms exist to control resource utilization of systems that are susceptible to Denial of Service (DoS) attacks to limit and prioritize the use of resources.	5	NIST SP 800-53B R5 Baseline: Not Selected	SC-5(2)	SC-5(2)	SC-5(2)	SC-5(2)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)	Low	Mod	High	Privacy
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 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	NIST SP 800-53B R5 Baseline: Not Selected	SC-5(2)	SC-5(2)	SC-5(2)	SC-5(2)
SC-5(3)	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	NIST SP 800-53B R5 Baseline: Not Selected				
SC-6	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 systems that are susceptible to Denial of Service (DoS) attacks to limit and prioritize the use of resources.	5	NIST SP 800-53B R5 Baseline: Not Selected				
SC-7	Boundary Protection	a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system;b. Implement subnetworks for publicly accessible system components that are [Selection (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	NIST SP 800-53B R5 Baseline: Low	SC-7	SC-7	SC-7	
SC-7(1)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SC-7(2)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SC-7(3)	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 systems.	10	NIST SP 800-53B R5 Baseline: Moderate		SC-7(3)	SC-7(3)	
SC-7(4)	Boundary Protection | External Telecommunications Services	a. Implement a managed interface for each external telecommunication service;b. Establish a traffic flow policy for each managed interface;c. Protect the confidentiality and integrity of the information being transmitted across each interface;d. Document each exception to the traffic flow policy with a supporting mission or business need and duration of that need;e. Review exceptions to the traffic flow policy [Assignment: organization-defined frequency] and remove exceptions that are no longer supported by an explicit mission or business need;f. Prevent unauthorized exchange of control plane traffic with external networks;g. Publish information to enable remote networks to detect unauthorized control plane traffic from internal networks; 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	NIST SP 800-53B R5 Baseline: Moderate		SC-7(4)	SC-7(4)	
SC-7(5)	Boundary Protection | Deny by Default — Allow by Exception	Deny network communications traffic by default and allow network communications traffic by exception [Selection (one or more): at managed interfaces; for [Assignment: organization-defined systems]].	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	NIST SP 800-53B R5 Baseline: Moderate		SC-7(5)	SC-7(5)	
SC-7(6)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SC-7(7)	Boundary Protection | Split Tunneling for Remote Devices	Prevent split tunneling for remote devices connecting to organizational systems unless the split tunnel is securely provisioned using [Assignment: organization-defined safeguards].	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-	10	NIST SP 800-53B R5 Baseline: Moderate		SC-7(7)	SC-7(7)	
SC-7(8)	Boundary Protection | Route Traffic to Authenticated Proxy Servers	Route [Assignment: organization-defined internal communications traffic] to [Assignment: organization-defined external networks] through authenticated proxy servers at managed interfaces.	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	5	NIST SP 800-53B R5 Baseline: Moderate	SC-7(8)	SC-7(8)	SC-7(8)	SC-7(8)
SC-7(8)	Boundary Protection | Route Traffic to Authenticated Proxy Servers	Route [Assignment: organization-defined internal communications traffic] to [Assignment: organization-defined external networks] through authenticated proxy servers at managed interfaces.	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	NIST SP 800-53B R5 Baseline: Moderate	SC-7(8)	SC-7(8)	SC-7(8)	SC-7(8)
SC-7(9)	Boundary Protection | Restrict Threatening Outgoing Communications	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	5	NIST SP 800-53B R5 Baseline: Not Selected	SC-7(9)	SC-7(9)	SC-7(9)	SC-7(9)
SC-7(9)	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	NIST SP 800-53B R5 Baseline: Not Selected	SC-7(9)	SC-7(9)	SC-7(9)	SC-7(9)
SC-7(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	NIST SP 800-53B R5 Baseline: Not Selected	SC-7(10)	SC-7(10)	SC-7(10)	SC-7(10)
SC-7(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	5	NIST SP 800-53B R5 Baseline: Not Selected	SC-7(10)	SC-7(10)	SC-7(10)	SC-7(10)
SC-7(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	NIST SP 800-53B R5 Baseline: Not Selected	SC-7(11)	SC-7(11)	SC-7(11)	SC-7(11)
SC-7(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	5	NIST SP 800-53B R5 Baseline: Not Selected	SC-7(11)	SC-7(11)	SC-7(11)	SC-7(11)
SC-7(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	NIST SP 800-53B R5 Baseline: Not Selected				
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 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	5	NIST SP 800-53B R5 Baseline: Not Selected				
SC-7(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	5	NIST SP 800-53B R5 Baseline: Not Selected	SC-7(14)	SC-7(14)	SC-7(14)	SC-7(14)
SC-7(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	NIST SP 800-53B R5 Baseline: Not Selected	SC-7(14)	SC-7(14)	SC-7(14)	SC-7(14)
SC-7(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,	5	NIST SP 800-53B R5 Baseline: Not Selected	SC-7(14)	SC-7(14)	SC-7(14)	SC-7(14)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)	Low	Mod	High	Privacy
SC-7(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	NIST SP 800-53B R5 Baseline: Not Selected				
SC-7(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	NIST SP 800-53B R5 Baseline: Not Selected				
SC-7(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	NIST SP 800-53B R5 Baseline: Not Selected				
SC-7(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 cybersecurity & data privacy practices in the specification, design, development, implementation and modification of	5	NIST SP 800-53B R5 Baseline: High			SC-7(18)	
SC-7(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	NIST SP 800-53B R5 Baseline: Not Selected				
SC-7(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	10	NIST SP 800-53B R5 Baseline: Not Selected				
SC-7(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 Information System Components	NET-03.7	Mechanisms exist to employ boundary protections to isolate systems, services and processes that support critical missions and/or	10	NIST SP 800-53B R5 Baseline: High			SC-7(21)	
SC-7(22)	Boundary Protection | Separate Subnets for Connecting to Different Security	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	NIST SP 800-53B R5 Baseline: Not Selected				
SC-7(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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SC-7(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	Functional	Equal	Personal Data (PD)	NET-03.4	Mechanisms exist to apply network-based processing rules to data elements of Personal Data (PD).	10	NIST SP 800-53B R5 Baseline: Not Selected				SC-7(24)
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].	Functional	Intersects With	System Interconnections	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, the interface characteristics, cybersecurity & data privacy requirements and the nature of the information communicated.	5	NIST SP 800-53B R5 Baseline: Not Selected				
SC-7(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	System Interconnections	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, the interface characteristics, cybersecurity & data privacy requirements and the nature of the information communicated.	5	NIST SP 800-53B R5 Baseline: Not Selected				
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].	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	NIST SP 800-53B R5 Baseline: Not Selected				
SC-7(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	10	NIST SP 800-53B R5 Baseline: Not Selected				
SC-7(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	NIST SP 800-53B R5 Baseline: Not Selected	SC-7(29)	SC-7(29)	SC-7(29)	SC-7(29)
SC-7(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	5	NIST SP 800-53B R5 Baseline: Not Selected	SC-7(29)	SC-7(29)	SC-7(29)	SC-7(29)
SC-7(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	NIST SP 800-53B R5 Baseline: Not Selected	SC-7(29)	SC-7(29)	SC-7(29)	SC-7(29)
SC-8	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	NIST SP 800-53B R5 Baseline: Moderate	SC-8	SC-8	SC-8	SC-8
SC-8	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	NIST SP 800-53B R5 Baseline: Moderate	SC-8	SC-8	SC-8	SC-8
SC-8(1)	Transmission Confidentiality and Integrity | Cryptographic	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	NIST SP 800-53B R5 Baseline: Moderate	SC-8(1)	SC-8(1)	SC-8(1)	SC-8(1)
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.	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	NIST SP 800-53B R5 Baseline: Moderate	SC-8(1)	SC-8(1)	SC-8(1)	SC-8(1)
SC-8(1)	Transmission Confidentiality and Integrity | Cryptographic	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	NIST SP 800-53B R5 Baseline: Moderate	SC-8(1)	SC-8(1)	SC-8(1)	SC-8(1)
SC-8(2)	Transmission Confidentiality and Integrity | Pre- and Post-transmission	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	5	NIST SP 800-53B R5 Baseline: Not Selected	SC-8(2)	SC-8(2)	SC-8(2)	SC-8(2)
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.	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	NIST SP 800-53B R5 Baseline: Not Selected	SC-8(2)	SC-8(2)	SC-8(2)	SC-8(2)
SC-8(2)	Transmission Confidentiality and Integrity | Pre- and Post-transmission	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	NIST SP 800-53B R5 Baseline: Not Selected	SC-8(2)	SC-8(2)	SC-8(2)	SC-8(2)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)	Low	Mod	High	Privacy
SC-8(3)	Transmission Confidentiality and Integrity | Cryptographic Protection for	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	NIST SP 800-53B R5 Baseline: Not Selected				
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].	Functional	Equal	Conceal / Randomize Communications	CRY-01.4	Cryptographic mechanisms exist to conceal or randomize communication patterns.	10	NIST SP 800-53B R5 Baseline: Not Selected				
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.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SC-9	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	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	NIST SP 800-53B R5 Baseline: Moderate		SC-10	SC-10	
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	NIST SP 800-53B R5 Baseline: Not Selected				
SC-11(1)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: 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	NIST SP 800-53B R5 Baseline: Low	SC-12	SC-12	SC-12	
SC-12(1)	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	NIST SP 800-53B R5 Baseline: High			SC-12(1)	
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.	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	NIST SP 800-53B R5 Baseline: Not Selected				
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; 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	NIST SP 800-53B R5 Baseline: Not Selected				
SC-12(4)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SC-12(5)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SC-12(6)	Cryptographic Key Establishment and Management | Physical Control of	Maintain physical control of cryptographic keys when stored information is encrypted by external service providers.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: 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	NIST SP 800-53B R5 Baseline: Low	SC-13	SC-13	SC-13	SC-13
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	NIST SP 800-53B R5 Baseline: Low	SC-13	SC-13	SC-13	SC-13
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	NIST SP 800-53B R5 Baseline: Low	SC-13	SC-13	SC-13	SC-13
SC-13(1)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SC-13(2)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SC-13(3)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SC-13(4)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SC-14	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	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	5	NIST SP 800-53B R5 Baseline: Low	SC-15	SC-15	SC-15	
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.	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	5	NIST SP 800-53B R5 Baseline: Not Selected				
SC-15(2)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SC-15(3)	Collaborative Computing Devices and Applications | Disabling and Removal in Secure	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 information systems and secure work areas.	10	NIST SP 800-53B R5 Baseline: Not Selected				
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].	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	NIST SP 800-53B R5 Baseline: 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 Privacy Attributes	CRY-10	Mechanisms exist to ensure systems associate security attributes with information exchanged between systems.	5	NIST SP 800-53B R5 Baseline: Not Selected				
SC-16(1)	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	NIST SP 800-53B R5 Baseline: Not Selected	SC-16(1)	SC-16(1)	SC-16(1)	SC-16(1)
SC-16(1)	Transmission of Security and Privacy Attributes | Integrity Verification	Verify the integrity of transmitted security and privacy attributes.	Functional	Intersects With	Transmission of Cybersecurity & Data Privacy Attributes	CRY-10	Mechanisms exist to ensure systems associate security attributes with information exchanged between systems.	5	NIST SP 800-53B R5 Baseline: Not Selected	SC-16(1)	SC-16(1)	SC-16(1)	SC-16(1)
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 process.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: 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 (optional)	Notes (optional)	Low	Mod	High	Privacy
SC-16(3)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: 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	NIST SP 800-53B R5 Baseline: Moderate		SC-17	SC-17	
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	NIST SP 800-53B R5 Baseline: Moderate		SC-18	SC-18	
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].	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	NIST SP 800-53B R5 Baseline: Not Selected	SC-18(1)	SC-18(1)	SC-18(1)	SC-18(1)
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].	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	5	NIST SP 800-53B R5 Baseline: Not Selected	SC-18(1)	SC-18(1)	SC-18(1)	SC-18(1)
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].	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	NIST SP 800-53B R5 Baseline: Not Selected	SC-18(1)	SC-18(1)	SC-18(1)	SC-18(1)
SC-18(2)	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	NIST SP 800-53B R5 Baseline: Not Selected	SC-18(2)	SC-18(2)	SC-18(2)	SC-18(2)
SC-18(2)	Mobile Code | Acquisition, Development, and	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	NIST SP 800-53B R5 Baseline: Not Selected	SC-18(2)	SC-18(2)	SC-18(2)	SC-18(2)
SC-18(3)	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	NIST SP 800-53B R5 Baseline: Not Selected	SC-18(3)	SC-18(3)	SC-18(3)	SC-18(3)
SC-18(3)	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	NIST SP 800-53B R5 Baseline: Not Selected	SC-18(3)	SC-18(3)	SC-18(3)	SC-18(3)
SC-18(4)	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	NIST SP 800-53B R5 Baseline: Not Selected	SC-18(4)	SC-18(4)	SC-18(4)	SC-18(4)
SC-18(4)	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	NIST SP 800-53B R5 Baseline: Not Selected	SC-18(4)	SC-18(4)	SC-18(4)	SC-18(4)
SC-18(5)	Mobile Code | Allow Execution Only in Confined	Allow execution of permitted mobile code only in confined virtual machine environments.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SC-19	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	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; andb. 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	NIST SP 800-53B R5 Baseline: Low	SC-20	SC-20	SC-20	
SC-20(1)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SC-20(2)	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	NIST SP 800-53B R5 Baseline: 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	10	NIST SP 800-53B R5 Baseline: Low	SC-21	SC-21	SC-21	
SC-21(1)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	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	10	NIST SP 800-53B R5 Baseline: Low	SC-22	SC-22	SC-22	
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	NIST SP 800-53B R5 Baseline: Moderate		SC-23	SC-23	
SC-23(1)	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	10	NIST SP 800-53B R5 Baseline: Not Selected				
SC-23(2)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SC-23(3)	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	NIST SP 800-53B R5 Baseline: Not Selected				
SC-23(4)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SC-23(5)	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	NIST SP 800-53B R5 Baseline: 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	NIST SP 800-53B R5 Baseline: High			SC-24	
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	NIST SP 800-53B R5 Baseline: 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	10	NIST SP 800-53B R5 Baseline: Not Selected				
SC-26(1)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	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	NIST SP 800-53B R5 Baseline: 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	NIST SP 800-53B R5 Baseline: Moderate	SC-28	SC-28	SC-28	SC-28
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	NIST SP 800-53B R5 Baseline: Moderate	SC-28	SC-28	SC-28	SC-28

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)	Low	Mod	High	Privacy
SC-28(1)	Protection of Information at Rest | Cryptographic Protection	Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information].	Functional	Intersects With	Cryptographic Protection	BCD-11.4	Cryptographic mechanisms exist to prevent the unauthorized disclosure and/or modification of backup information.	5	NIST SP 800-53B R5 Baseline: Moderate	SC-28(1)	SC-28(1)	SC-28(1)	SC-28(1)
SC-28(1)	Protection of Information at Rest | Cryptographic Protection	Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information].	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	NIST SP 800-53B R5 Baseline: Moderate	SC-28(1)	SC-28(1)	SC-28(1)	SC-28(1)
SC-28(1)	Protection of Information at Rest | Cryptographic Protection	Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information].	Functional	Intersects With	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	5	NIST SP 800-53B R5 Baseline: Moderate	SC-28(1)	SC-28(1)	SC-28(1)	SC-28(1)
SC-28(1)	Protection of Information at Rest | Cryptographic Protection	Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information].	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	NIST SP 800-53B R5 Baseline: Moderate	SC-28(1)	SC-28(1)	SC-28(1)	SC-28(1)
SC-28(2)	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	NIST SP 800-53B R5 Baseline: Not Selected	SC-28(2)	SC-28(2)	SC-28(2)	SC-28(2)
SC-28(2)	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 satisfying Recovery Time Objectives (RTOs) and Recovery Point Objectives	5	NIST SP 800-53B R5 Baseline: Not Selected	SC-28(2)	SC-28(2)	SC-28(2)	SC-28(2)
SC-28(3)	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	NIST SP 800-53B R5 Baseline: 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	10	NIST SP 800-53B R5 Baseline: Not Selected				
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].	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	NIST SP 800-53B R5 Baseline: 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 systems to confuse and mislead adversaries.	5	NIST SP 800-53B R5 Baseline: Not Selected				
SC-30(1)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SC-30(2)	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	NIST SP 800-53B R5 Baseline: Not Selected				
SC-30(3)	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	NIST SP 800-53B R5 Baseline: Not Selected				
SC-30(4)	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 systems to confuse and mislead adversaries.	5	NIST SP 800-53B R5 Baseline: Not Selected				
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].	Functional	Intersects With	Concealment & Misdirection	SEA-14	Mechanisms exist to utilize concealment and misdirection techniques for systems to confuse and mislead adversaries.	5	NIST SP 800-53B R5 Baseline: 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	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	NIST SP 800-53B R5 Baseline: Not Selected				
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.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
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].	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
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 environment of the system.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: 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	NIST SP 800-53B R5 Baseline: Not Selected				
SC-32(1)	System Partitioning | Separate Physical Domains for Privileged Functions	Partition privileged functions into separate physical domains.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SC-33	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	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	NIST SP 800-53B R5 Baseline: Not Selected				
SC-34(1)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SC-34(2)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SC-34(3)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	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	NIST SP 800-53B R5 Baseline: 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	NIST SP 800-53B R5 Baseline: Not Selected				
SC-36(1)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SC-36(2)	Distributed Processing and Storage |	Synchronize the following duplicate systems or system components: [Assignment: organization-defined duplicate systems or system components].	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: 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 (optional)	Notes (optional)	Low	Mod	High	Privacy
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	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	5	NIST SP 800-53B R5 Baseline: Not Selected				
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].	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	5	NIST SP 800-53B R5 Baseline: 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	NIST SP 800-53B R5 Baseline: Not Selected	SC-38	SC-38	SC-38	SC-38
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	NIST SP 800-53B R5 Baseline: Not Selected	SC-38	SC-38	SC-38	SC-38
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	NIST SP 800-53B R5 Baseline: Low	SC-39	SC-39	SC-39	
SC-39(1)	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	NIST SP 800-53B R5 Baseline: Not Selected				
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].	Functional	Equal	Thread Separation	SEA-04.3	Mechanisms exist to maintain a separate execution domain for each thread in multi-threaded processing.	10	NIST SP 800-53B R5 Baseline: 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	5	NIST SP 800-53B R5 Baseline: Not Selected	SC-40	SC-40	SC-40	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].	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	NIST SP 800-53B R5 Baseline: Not Selected	SC-40	SC-40	SC-40	SC-40
SC-40(1)	Wireless Link Protection | Electromagnetic	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SC-40(2)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
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.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SC-40(4)	Wireless Link Protection | Signal Parameter	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: 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	NIST SP 800-53B R5 Baseline: 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	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	NIST SP 800-53B R5 Baseline: Not Selected				
SC-42(1)	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	NIST SP 800-53B R5 Baseline: Not Selected				
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].	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	10	NIST SP 800-53B R5 Baseline: Not Selected				
SC-42(3)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SC-42(4)	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	NIST SP 800-53B R5 Baseline: Not Selected				
SC-42(5)	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	NIST SP 800-53B R5 Baseline: 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	NIST SP 800-53B R5 Baseline: 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	10	NIST SP 800-53B R5 Baseline: 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	NIST SP 800-53B R5 Baseline: Not Selected				
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]; andb. Synchronize the internal system clocks to the authoritative time source when the time difference is greater than [Assignment: organization-	Functional	Equal	Synchronization With Authoritative Time Source	MON-07.1	Mechanisms exist to synchronize internal system clocks with an authoritative time source.	10	NIST SP 800-53B R5 Baseline: Not Selected				
SC-45(2)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: 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	NIST SP 800-53B R5 Baseline: 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	NIST SP 800-53B R5 Baseline: 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 (optional)	Notes (optional)	Low	Mod	High	Privacy
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	NIST SP 800-53B R5 Baseline: Not Selected	SC-48	SC-48	SC-48	SC-48
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	NIST SP 800-53B R5 Baseline: Not Selected	SC-48	SC-48	SC-48	SC-48
SC-48(1)	Sensor Relocation | Dynamic Relocation of Sensors or Monitoring	Dynamically relocate [Assignment: organization-defined sensors and monitoring capabilities] to [Assignment: organization-defined locations] under the following conditions or circumstances: [Assignment: organization-defined	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: 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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: 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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SI-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and information integrity policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 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-	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	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 continuing suitability, adequacy and effectiveness.	5	NIST SP 800-53B R5 Baseline: Low	SI-1	SI-1	SI-1	SI-1
SI-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and information integrity policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 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-	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity & data privacy practices in the specification, design, development, implementation and modification of systems and services.	10	NIST SP 800-53B R5 Baseline: Low	SI-1	SI-1	SI-1	SI-1
SI-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and information integrity policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 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-	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	NIST SP 800-53B R5 Baseline: Low	SI-1	SI-1	SI-1	SI-1
SI-2	Flaw Remediation	a. Identify, report, and correct system flaws;b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;c. Install security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates; 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	NIST SP 800-53B R5 Baseline: Low	SI-2	SI-2	SI-2	SI-2
SI-2	Flaw Remediation	a. Identify, report, and correct system flaws;b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;c. Install security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates; 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 operating systems, applications and firmware.	5	NIST SP 800-53B R5 Baseline: Low	SI-2	SI-2	SI-2	SI-2
SI-2	Flaw Remediation	a. Identify, report, and correct system flaws;b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;c. Install security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates; andd. Incorporate flaw remediation into the organizational configuration management process.	Functional	Intersects With	Automatic Antimalware Signature Updates	END-04.1	Mechanisms exist to automatically update antimalware technologies, including signature definitions.	5	NIST SP 800-53B R5 Baseline: Low	SI-2	SI-2	SI-2	SI-2
SI-2(1)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SI-2(2)	Flaw Remediation | Automated Flaw Remediation Status	Determine if system components have applicable security-relevant software and firmware updates installed using [Assignment: organization-defined automated mechanisms] [Assignment: organization-defined frequency].	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	NIST SP 800-53B R5 Baseline: Moderate		SI-2(2)	SI-2(2)	
SI-2(3)	Flaw Remediation | Time to Remediate Flaws and Benchmarks for	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	NIST SP 800-53B R5 Baseline: Not Selected				
SI-2(4)	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	NIST SP 800-53B R5 Baseline: Not Selected	SI-2(4)	SI-2(4)	SI-2(4)	SI-2(4)
SI-2(4)	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	NIST SP 800-53B R5 Baseline: Not Selected	SI-2(4)	SI-2(4)	SI-2(4)	SI-2(4)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)	Low	Mod	High	Privacy
SI-2(4)	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	VPM-05.1	Mechanisms exist to centrally-manage the flaw remediation process.	5	NIST SP 800-53B R5 Baseline: Not Selected	SI-2(4)	SI-2(4)	SI-2(4)	SI-2(4)
SI-2(4)	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 operating systems, applications and	5	NIST SP 800-53B R5 Baseline: Not Selected	SI-2(4)	SI-2(4)	SI-2(4)	SI-2(4)
SI-2(5)	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	NIST SP 800-53B R5 Baseline: Not Selected				
SI-2(6)	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	NIST SP 800-53B R5 Baseline: Not Selected				
SI-3	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 operating systems, applications and firmware.	5	NIST SP 800-53B R5 Baseline: Low	SI-3	SI-3	SI-3	SI-3
SI-3	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	NIST SP 800-53B R5 Baseline: Low	SI-3	SI-3	SI-3	SI-3
SI-3	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	NIST SP 800-53B R5 Baseline: Low	SI-3	SI-3	SI-3	SI-3
SI-3	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	NIST SP 800-53B R5 Baseline: Low	SI-3	SI-3	SI-3	SI-3
SI-3	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	NIST SP 800-53B R5 Baseline: Low	SI-3	SI-3	SI-3	SI-3

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)	Low	Mod	High	Privacy
SI-3	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	Mechanisms exist to automatically update antimalware technologies, including signature definitions.	5	NIST SP 800-53B R5 Baseline: Low	SI-3	SI-3	SI-3	SI-3
SI-3	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	NIST SP 800-53B R5 Baseline: Low	SI-3	SI-3	SI-3	SI-3
SI-3(1)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SI-3(2)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SI-3(3)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SI-3(4)	Malicious Code Protection | Updates Only by Privileged	Update malicious code protection mechanisms only when directed by a privileged user.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SI-3(5)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SI-3(6)	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	10	NIST SP 800-53B R5 Baseline: Not Selected				
SI-3(7)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SI-3(8)	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;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SI-3(9)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SI-3(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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SI-4	System Monitoring	a. Monitor the system to detect:1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]; 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:	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	NIST SP 800-53B R5 Baseline: Low	SI-4	SI-4	SI-4	SI-4
SI-4	System Monitoring	a. Monitor the system to detect:1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]; 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:	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	NIST SP 800-53B R5 Baseline: Low	SI-4	SI-4	SI-4	SI-4
SI-4	System Monitoring	a. Monitor the system to detect:1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]; 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:	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	NIST SP 800-53B R5 Baseline: Low	SI-4	SI-4	SI-4	SI-4

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)	Low	Mod	High	Privacy
SI-4	System Monitoring	a. Monitor the system to detect:1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]; 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:	Functional	Intersects With	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	5	NIST SP 800-53B R5 Baseline: Low	SI-4	SI-4	SI-4	SI-4
SI-4(1)	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	NIST SP 800-53B R5 Baseline: Not Selected				
SI-4(2)	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	NIST SP 800-53B R5 Baseline: Moderate		SI-4(2)	SI-4(2)	
SI-4(3)	System Monitoring | Automated Tool and Mechanism	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SI-4(4)	System Monitoring | Inbound and Outbound Communications Traffic	a. Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic;b. Monitor inbound and outbound communications traffic [Assignment: organization-defined frequency] for [Assignment: organization-defined unusual or unauthorized activities or conditions].	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	NIST SP 800-53B R5 Baseline: Moderate		SI-4(4)	SI-4(4)	
SI-4(5)	System Monitoring | System-generated Alerts	Alert [Assignment: organization-defined personnel or roles] when the following system-generated indications of compromise or potential compromise occur: [Assignment: organization-defined compromise indicators].	Functional	Equal	System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data privacy and supply chain activities to achieve integrated	10	NIST SP 800-53B R5 Baseline: Moderate		SI-4(5)	SI-4(5)	
SI-4(6)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SI-4(7)	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	Mechanisms exist to automatically implement pre-determined corrective actions in response to detected events that have security incident implications.	5	NIST SP 800-53B R5 Baseline: Not Selected	SI-4(7)	SI-4(7)	SI-4(7)	SI-4(7)
SI-4(7)	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	NIST SP 800-53B R5 Baseline: Not Selected	SI-4(7)	SI-4(7)	SI-4(7)	SI-4(7)
SI-4(8)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SI-4(9)	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	NIST SP 800-53B R5 Baseline: Not Selected				
SI-4(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	NIST SP 800-53B R5 Baseline: High			SI-4(10)	
SI-4(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 detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	10	NIST SP 800-53B R5 Baseline: Not Selected				
SI-4(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	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	NIST SP 800-53B R5 Baseline: High	SI-4(12)	SI-4(12)	SI-4(12)	SI-4(12)
SI-4(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	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	NIST SP 800-53B R5 Baseline: High	SI-4(12)	SI-4(12)	SI-4(12)	SI-4(12)
SI-4(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	NIST SP 800-53B R5 Baseline: Not Selected				
SI-4(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 Intrusion Detection System (WIDS)	MON-01.5	Mechanisms exist to utilize Wireless Intrusion Detection / Protection Systems (WIDS / WIPS) to identify rogue wireless devices and to detect attack attempts via wireless	5	NIST SP 800-53B R5 Baseline: High			SI-4(14)	
SI-4(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 System (WIDS)	MON-01.5	Mechanisms exist to utilize Wireless Intrusion Detection / Protection Systems (WIDS / WIPS) to identify rogue wireless devices and to detect attack attempts via wireless	5	NIST SP 800-53B R5 Baseline: Not Selected				
SI-4(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	10	NIST SP 800-53B R5 Baseline: Not Selected				
SI-4(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	10	NIST SP 800-53B R5 Baseline: Not Selected				
SI-4(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	5	NIST SP 800-53B R5 Baseline: Not Selected	SI-4(18)	SI-4(18)	SI-4(18)	SI-4(18)
SI-4(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	NIST SP 800-53B R5 Baseline: Not Selected	SI-4(18)	SI-4(18)	SI-4(18)	SI-4(18)
SI-4(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	NIST SP 800-53B R5 Baseline: Not Selected				
SI-4(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	NIST SP 800-53B R5 Baseline: High			SI-4(20)	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)	Low	Mod	High	Privacy
SI-4(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	NIST SP 800-53B R5 Baseline: Not Selected				
SI-4(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	NIST SP 800-53B R5 Baseline: High			SI-4(22)	
SI-4(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	10	NIST SP 800-53B R5 Baseline: Not Selected				
SI-4(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	NIST SP 800-53B R5 Baseline: Not Selected	SI-4(24)	SI-4(24)	SI-4(24)	SI-4(24)
SI-4(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 assets to generate alerts for unauthorized modifications.	5	NIST SP 800-53B R5 Baseline: Not Selected	SI-4(24)	SI-4(24)	SI-4(24)	SI-4(24)
SI-4(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 systems.	5	NIST SP 800-53B R5 Baseline: Not Selected	SI-4(25)	SI-4(25)	SI-4(25)	SI-4(25)
SI-4(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	NIST SP 800-53B R5 Baseline: Not Selected	SI-4(25)	SI-4(25)	SI-4(25)	SI-4(25)
SI-5	Security Alerts, Advisories, and Directives	a. Receive system security alerts, advisories, and directives from [Assignment: organization-defined external organizations] on an ongoing basis;b. Generate internal security alerts, advisories, and directives as deemed necessary;c. Disseminate security alerts, advisories, and directives to: [Selection (one or more): [Assignment: organization-defined personnel or roles]; [Assignment: organization-defined elements within the organization]; [Assignment: organization-defined external organizations]]; 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	NIST SP 800-53B R5 Baseline: Low	SI-5	SI-5	SI-5	SI-5
SI-5	Security Alerts, Advisories, and Directives	a. Receive system security alerts, advisories, and directives from [Assignment: organization-defined external organizations] on an ongoing basis;b. Generate internal security alerts, advisories, and directives as deemed necessary;c. Disseminate security alerts, advisories, and directives to: [Selection (one or more): [Assignment: organization-defined personnel or roles]; [Assignment: organization-defined elements within the organization]; [Assignment: organization-defined external organizations]]; 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 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	NIST SP 800-53B R5 Baseline: Low	SI-5	SI-5	SI-5	SI-5
SI-5	Security Alerts, Advisories, and Directives	a. Receive system security alerts, advisories, and directives from [Assignment: organization-defined external organizations] on an ongoing basis;b. Generate internal security alerts, advisories, and directives as deemed necessary;c. Disseminate security alerts, advisories, and directives to: [Selection (one or more): [Assignment: organization-defined personnel or roles]; [Assignment: organization-defined elements within the organization]; [Assignment: organization-defined external organizations]]; 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	NIST SP 800-53B R5 Baseline: Low	SI-5	SI-5	SI-5	SI-5
SI-5(1)	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 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	5	NIST SP 800-53B R5 Baseline: High			SI-5(1)	
SI-6	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	Functional	Intersects With	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.	5	NIST SP 800-53B R5 Baseline: High			SI-6	
SI-6(1)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SI-6(2)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SI-6(3)	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 cybersecurity & data privacy function verification to appropriate organizational	10	NIST SP 800-53B R5 Baseline: Not Selected				
SI-7	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	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	NIST SP 800-53B R5 Baseline: Moderate	SI-7	SI-7	SI-7	SI-7
SI-7	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	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	NIST SP 800-53B R5 Baseline: Moderate	SI-7	SI-7	SI-7	SI-7
SI-7	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	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	NIST SP 800-53B R5 Baseline: Moderate	SI-7	SI-7	SI-7	SI-7
SI-7(1)	Software, Firmware, and Information Integrity | Integrity Checks	Perform an integrity check of [Assignment: organization-defined software, firmware, and information] [Selection (one or more): at startup; at [Assignment: organization-defined transitional states or security-relevant events]; [Assignment: organization-defined frequency]].	Functional	Equal	Integrity Checks	END-06.1	Mechanisms exist to validate configurations through integrity checking of software and firmware.	10	NIST SP 800-53B R5 Baseline: Moderate		SI-7(1)	SI-7(1)	
SI-7(2)	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	NIST SP 800-53B R5 Baseline: High			SI-7(2)	
SI-7(3)	Software, Firmware, and Information Integrity | Centrally Managed Integrity	Employ centrally managed integrity verification tools.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: 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 (optional)	Notes (optional)	Low	Mod	High	Privacy
SI-7(4)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SI-7(5)	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	NIST SP 800-53B R5 Baseline: High			SI-7(5)	
SI-7(6)	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	NIST SP 800-53B R5 Baseline: Not Selected				
SI-7(7)	Software, Firmware, and Information Integrity | Integration of Detection and Response	Incorporate the detection of the following unauthorized changes into the organizational incident response capability: [Assignment: organization-defined security-relevant changes to the system].	Functional	Equal	Endpoint Detection & Response (EDR)	END-06.2	Mechanisms exist to detect and respond to unauthorized configuration changes as cybersecurity incidents.	10	NIST SP 800-53B R5 Baseline: Moderate		SI-7(7)	SI-7(7)	
SI-7(8)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SI-7(9)	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 information systems.	10	NIST SP 800-53B R5 Baseline: Not Selected				
SI-7(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 information systems.	10	NIST SP 800-53B R5 Baseline: Not Selected				
SI-7(11)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SI-7(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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SI-7(13)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SI-7(14)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SI-7(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	NIST SP 800-53B R5 Baseline: High			SI-7(15)	
SI-7(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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SI-7(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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SI-8	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	NIST SP 800-53B R5 Baseline: Moderate		SI-8	SI-8	
SI-8(1)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SI-8(2)	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	NIST SP 800-53B R5 Baseline: Moderate		SI-8(2)	SI-8(2)	
SI-8(3)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SI-9	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	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	NIST SP 800-53B R5 Baseline: Moderate	SI-10	SI-10	SI-10	SI-10
SI-10	Information Input Validation	Check the validity of the following information inputs: [Assignment: organization-defined information inputs to the	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	NIST SP 800-53B R5 Baseline: Moderate	SI-10	SI-10	SI-10	SI-10
SI-10(1)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SI-10(2)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SI-10(3)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SI-10(4)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SI-10(5)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SI-10(6)	Information Input Validation | Injection Prevention	Prevent untrusted data injections.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: 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	NIST SP 800-53B R5 Baseline: Moderate		SI-11	SI-11	
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	NIST SP 800-53B R5 Baseline: Low	SI-12	SI-12	SI-12	SI-12

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)	Low	Mod	High	Privacy
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	NIST SP 800-53B R5 Baseline: Low	SI-12	SI-12	SI-12	SI-12
SI-12(1)	Information Management and Retention | Limit Personally Identifiable Information Elements	Limit personally identifiable information being processed in the information life cycle to the following elements of personally identifiable information: [Assignment: organization-defined elements of personally identifiable information].	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	5	NIST SP 800-53B R5 Baseline: Not Selected	SI-12(1)	SI-12(1)	SI-12(1)	SI-12(1)
SI-12(1)	Information Management and Retention | Limit Personally Identifiable Information Elements	Limit personally identifiable information being processed in the information life cycle to the following elements of personally identifiable information: [Assignment: organization-defined elements of personally identifiable information].	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 business processes.	5	NIST SP 800-53B R5 Baseline: Not Selected	SI-12(1)	SI-12(1)	SI-12(1)	SI-12(1)
SI-12(2)	Information Management and Retention | Minimize Personally Identifiable Information in Testing, Training, and	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	NIST SP 800-53B R5 Baseline: Not Selected	SI-12(2)	SI-12(2)	SI-12(2)	SI-12(2)
SI-12(2)	Information Management and Retention | Minimize Personally Identifiable Information in Testing, Training, and Research	Use the following techniques to minimize the use of personally identifiable information for research, testing, or training: [Assignment: organization-defined techniques].	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	5	NIST SP 800-53B R5 Baseline: Not Selected	SI-12(2)	SI-12(2)	SI-12(2)	SI-12(2)
SI-12(3)	Information Management and Retention | Information Disposal	Use the following techniques to dispose of, destroy, or erase information following the retention period: [Assignment: organization-defined techniques].	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	NIST SP 800-53B R5 Baseline: Not Selected	SI-12(3)	SI-12(3)	SI-12(3)	SI-12(3)
SI-12(3)	Information Management and Retention | Information Disposal	Use the following techniques to dispose of, destroy, or erase information following the retention period: [Assignment: organization-defined techniques].	Functional	Intersects With	Information Disposal	DCH-21	Mechanisms exist to securely dispose of, destroy or erase information.	5	NIST SP 800-53B R5 Baseline: Not Selected	SI-12(3)	SI-12(3)	SI-12(3)	SI-12(3)
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	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 systems, applications and/or services.	5	NIST SP 800-53B R5 Baseline: Not Selected	SI-13	SI-13	SI-13	SI-13
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	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	NIST SP 800-53B R5 Baseline: Not Selected	SI-13	SI-13	SI-13	SI-13
SI-13(1)	Predictable Failure Prevention | Transferring Component	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SI-13(2)	Withdrawn	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0	Withdrawn				
SI-13(3)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SI-13(4)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SI-13(5)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: 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	NIST SP 800-53B R5 Baseline: Not Selected				
SI-14(1)	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 information system component and service refreshes are obtained from trusted sources.	10	NIST SP 800-53B R5 Baseline: Not Selected				
SI-14(2)	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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
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].	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: 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	NIST SP 800-53B R5 Baseline: 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	NIST SP 800-53B R5 Baseline: Moderate		SI-16	SI-16	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)	Low	Mod	High	Privacy
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	NIST SP 800-53B R5 Baseline: 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	NIST SP 800-53B R5 Baseline: Not Selected				SI-18
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].	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	NIST SP 800-53B R5 Baseline: Not Selected				
SI-18(2)	Personally Identifiable Information Quality Operations | Data	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	10	NIST SP 800-53B R5 Baseline: Not Selected				
SI-18(3)	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	NIST SP 800-53B R5 Baseline: Not Selected				
SI-18(4)	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	PRI-06.1	Mechanisms exist to establish and implement 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	5	NIST SP 800-53B R5 Baseline: Not Selected	SI-18(4)	SI-18(4)	SI-18(4)	SI-18(4)
SI-18(4)	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	NIST SP 800-53B R5 Baseline: Not Selected	SI-18(4)	SI-18(4)	SI-18(4)	SI-18(4)
SI-18(4)	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 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	NIST SP 800-53B R5 Baseline: Not Selected	SI-18(4)	SI-18(4)	SI-18(4)	SI-18(4)
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.	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	NIST SP 800-53B R5 Baseline: Not Selected	SI-18(5)	SI-18(5)	SI-18(5)	SI-18(5)
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.	Functional	Intersects With	Correcting Inaccurate Personal Data	PRI-06.1	Mechanisms exist to establish and implement 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	5	NIST SP 800-53B R5 Baseline: Not Selected	SI-18(5)	SI-18(5)	SI-18(5)	SI-18(5)
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.	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 or amended.	5	NIST SP 800-53B R5 Baseline: Not Selected	SI-18(5)	SI-18(5)	SI-18(5)	SI-18(5)
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	NIST SP 800-53B R5 Baseline: Not Selected				SI-19
SI-19(1)	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	NIST SP 800-53B R5 Baseline: Not Selected	SI-19(1)	SI-19(1)	SI-19(1)	SI-19(1)
SI-19(1)	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	NIST SP 800-53B R5 Baseline: Not Selected	SI-19(1)	SI-19(1)	SI-19(1)	SI-19(1)
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.	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	10	NIST SP 800-53B R5 Baseline: Not Selected				
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.	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	NIST SP 800-53B R5 Baseline: Not Selected				
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.	Functional	Intersects With	Data Masking	PRI-05.3	Mechanisms exist to mask sensitive/regulated data through data anonymization, pseudonymization, redaction or de-identification.	5	NIST SP 800-53B R5 Baseline: Not Selected	SI-19(4)	SI-19(4)	SI-19(4)	SI-19(4)
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.	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	NIST SP 800-53B R5 Baseline: Not Selected	SI-19(4)	SI-19(4)	SI-19(4)	SI-19(4)
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.	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	NIST SP 800-53B R5 Baseline: Not Selected				
SI-19(6)	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	NIST SP 800-53B R5 Baseline: Not Selected				
SI-19(7)	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	NIST SP 800-53B R5 Baseline: 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 (optional)	Notes (optional)	Low	Mod	High	Privacy
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 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	NIST SP 800-53B R5 Baseline: 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	NIST SP 800-53B R5 Baseline: 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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: 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	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: 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	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
SR-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] supply chain risk management policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 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	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	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 continuing suitability, adequacy and effectiveness.	5	NIST SP 800-53B R5 Baseline: Low	SR-1	SR-1	SR-1	SR-1
SR-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] supply chain risk management policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 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	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	NIST SP 800-53B R5 Baseline: Low	SR-1	SR-1	SR-1	SR-1
SR-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] supply chain risk management policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 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	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	NIST SP 800-53B R5 Baseline: Low	SR-1	SR-1	SR-1	SR-1
SR-2	Supply Chain Risk Management Plan	a. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the following systems, system components or system services: [Assignment: organization-defined systems, system components, or system services];b. Review and update the supply chain risk management plan [Assignment: organization-defined frequency] or as required, to address threat, organizational or environmental changes; andc. Protect the supply chain risk management plan from unauthorized	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 systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	5	NIST SP 800-53B R5 Baseline: Low	SR-2	SR-2	SR-2	SR-2
SR-2	Supply Chain Risk Management Plan	a. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the following systems, system components or system services: [Assignment: organization-defined systems, system components, or system services];b. Review and update the supply chain risk management plan [Assignment: organization-defined frequency] or as required, to address threat, organizational or environmental changes; andc. Protect the supply chain risk management plan from unauthorized	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to: (1) Evaluate security risks and threats associated with the services and product supply chains; and (2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	5	NIST SP 800-53B R5 Baseline: Low	SR-2	SR-2	SR-2	SR-2
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].	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to: (1) Evaluate security risks and threats associated with the services and product supply chains; and (2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	5	NIST SP 800-53B R5 Baseline: Low	SR-2(1)	SR-2(1)	SR-2(1)	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)	Low	Mod	High	Privacy
SR-3	Supply Chain Controls and Processes	a. Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of [Assignment: organization-defined system or system component] in coordination with [Assignment: organization-defined supply chain personnel];b. Employ the following controls to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain-related events: [Assignment: organization-defined supply chain controls]; andc. Document the selected and implemented supply chain processes and controls in [Selection (one): security and privacy plans; supply chain risk management plan; [Assignment:	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	NIST SP 800-53B R5 Baseline: Low	SR-3	SR-3	SR-3	
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].	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	5	NIST SP 800-53B R5 Baseline: Not Selected	SR-3(1)	SR-3(1)	SR-3(1)	SR-3(1)
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].	Functional	Intersects With	Supplier Diversity	TDA-03.1	Mechanisms exist to obtain cybersecurity & data privacy technologies from different suppliers to minimize supply chain risk.	5	NIST SP 800-53B R5 Baseline: Not Selected	SR-3(1)	SR-3(1)	SR-3(1)	SR-3(1)
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].	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 systems, system components or services.	5	NIST SP 800-53B R5 Baseline: Not Selected	SR-3(1)	SR-3(1)	SR-3(1)	SR-3(1)
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 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	10	NIST SP 800-53B R5 Baseline: Not Selected				
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.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and	5	NIST SP 800-53B R5 Baseline: Not Selected	SR-3(3)	SR-3(3)	SR-3(3)	SR-3(3)
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.	Functional	Intersects With	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure cybersecurity & data privacy requirements are included in contracts that flow-down to applicable sub-contractors and	5	NIST SP 800-53B R5 Baseline: Not Selected	SR-3(3)	SR-3(3)	SR-3(3)	SR-3(3)
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].	Functional	Intersects With	Provenance	AST-03.2	Mechanisms exist to track the origin, development, ownership, location and changes to systems, system components and associated data.	5	NIST SP 800-53B R5 Baseline: Not Selected				
SR-4(1)	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 systems, system components and associated data.	5	NIST SP 800-53B R5 Baseline: Not Selected				
SR-4(2)	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 systems, system components and associated data.	5	NIST SP 800-53B R5 Baseline: Not Selected				
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].	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	NIST SP 800-53B R5 Baseline: Not Selected				
SR-4(4)	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	NIST SP 800-53B R5 Baseline: Not Selected				
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].	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 systems, system components or services.	5	NIST SP 800-53B R5 Baseline: Low	SR-5	SR-5	SR-5	
SR-5(1)	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	NIST SP 800-53B R5 Baseline: Not Selected				
SR-5(2)	Acquisition Strategies, Tools, and Methods | Assessments Prior to Selection, Acceptance,	Assess the system, system component, or system service prior to selection, acceptance, modification, or update.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	NIST SP 800-53B R5 Baseline: Not Selected				
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 [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 cybersecurity & data privacy controls.	5	NIST SP 800-53B R5 Baseline: Moderate		SR-6	SR-6	
SR-6(1)	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	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 cybersecurity & data privacy controls.	5	NIST SP 800-53B R5 Baseline: Not Selected				
SR-7	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 systems, system components and services, including documenting selected mitigating actions and monitoring performance against	5	NIST SP 800-53B R5 Baseline: Not Selected	SR-7	SR-7	SR-7	SR-7
SR-7	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	NIST SP 800-53B R5 Baseline: Not Selected	SR-7	SR-7	SR-7	SR-7
SR-8	Notification Agreements	Establish agreements and procedures with entities involved in the supply chain for the system, system component, or system service for the [Selection (one or more): notification of supply chain compromises; results of assessments or audits; [Assignment: organization-defined information]].	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 systems, applications and/or services that the	10	NIST SP 800-53B R5 Baseline: Low	SR-8	SR-8	SR-8	
SR-9	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 verify logical configuration settings and the physical integrity of critical technology assets throughout their	5	NIST SP 800-53B R5 Baseline: High			SR-9	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)	Low	Mod	High	Privacy
SR-9(1)	Tamper Resistance and Detection | Multiple Stages of System Development	Employ anti-tamper technologies, tools, and techniques throughout the system development life cycle.	Functional	Intersects With	Logical Tampering Protection	AST-15	Mechanisms exist to verify logical configuration settings and the physical integrity of critical technology assets throughout their	5	NIST SP 800-53B R5 Baseline: High			SR-9(1)	
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	NIST SP 800-53B R5 Baseline: Low	SR-10	SR-10	SR-10	SR-10
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	Functional	Intersects With	Inspection of Systems, Components & Devices	AST-15.1	Mechanisms exist to physically and logically inspect critical technology assets to detect evidence of tampering.	5	NIST SP 800-53B R5 Baseline: Low	SR-10	SR-10	SR-10	SR-10
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	NIST SP 800-53B R5 Baseline: Low	SR-11	SR-11	SR-11	
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).	Functional	Equal	Anti-Counterfeit Training	TDA-11.1	Mechanisms exist to train personnel to detect counterfeit system components, including hardware, software and firmware.	10	NIST SP 800-53B R5 Baseline: Low	SR-11(1)	SR-11(1)	SR-11(1)	
SR-11(2)	Component Authenticity | Configuration Control for Component Service and Repair	Maintain configuration control over the following system components awaiting service or repair and serviced or repaired components awaiting return to service: [Assignment: organization-defined system components].	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	NIST SP 800-53B R5 Baseline: Low	SR-11(2)	SR-11(2)	SR-11(2)	
SR-11(3)	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	NIST SP 800-53B R5 Baseline: 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	NIST SP 800-53B R5 Baseline: Low	SR-12	SR-12	SR-12	SR-12